

# FEDERAL BUREAU OF INVESTIGATION

*Uploaded 10/10/03*

**Precedence:** IMMEDIATE

**Date:** 09/12/2003

**To:** All Divisions

**Attn:** ADIC, AD, DAD, SAC, CDC

**From:** Office of the General Counsel  
National Security Law Branch

b2

b6

**Contact:** [REDACTED]

b7C

**Approved By:** Mueller Robert S III

**Drafted By:** [REDACTED]

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 12-08-2005 BY 55179/DMH/LP/RW 05-cv-0845

**Case ID #:** 66F-HQ-A1431182 *Serial 2*

**Title:** BUSINESS RECORD APPLICATIONS  
DELEGATION OF AUTHORITY

**Synopsis:** Delegates signature authority for Applications for Business Records to FBIHQ officials under 50 U.S.C. § 1861.

**Details:** The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C § 1861, provides for access to certain business records for foreign intelligence (FI) and international terrorism (IT) investigations through issuance of an order from the FISA Court (FISC). Section 1861(a) authorizes the "Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge)" to make an application for the order.

Thus, as permitted by 50 U.S.C. § 1861(a), I hereby designate certification signature authority for applications for FISA business records to the following FBI Officials:

1. The Deputy Director;
2. The Executive Assistant Director for Counterterrorism/Counterintelligence;
3. The Assistant Director and all Deputy Assistant Directors of the Counterterrorism, Counterintelligence, and Cyber Divisions; and
4. The General Counsel, the Deputy General Counsel for National Security Affairs, and the Senior Counsel for National Security Affairs.

To: All Divisions From: Office of the General Counsel  
Re: 66F-HQ-A1431182, 07/18/2003

The National Security Law Branch is hereby authorized to prepare business record applications and will issue guidance on the application process.

To: All Divisions From: Office of the General Counsel  
Re: 66F-HQ-A1431182, 07/18/2003

**LEAD:**

**Set Lead 1: (adm)**

ALL RECEIVING OFFICES

Disseminate to personnel involved in CI and IT operations and to other personnel as appropriate.

~~SECRET~~

DATE: 12-09-2005  
CLASSIFIED BY 65179/DMH/LP/PM 05-cv-0845  
REASON: 1.4 (c)  
DECLASSIFY ON: 12-09-2030

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

~~Secret~~

QUESTIONS FOR THE RECORD FROM DIRECTOR'S 5/20/04 SENATE HEARING  
NSLB RESPONSES

28. OGC. During the hearing, Senator Grassley asked you about the retroactive classification of information provided by the FBI to Committee staff related to a whistleblower who previously worked for the FBI translation program. I share Senator Grassley's concern that this order is unrealistic. A great deal of information regarding the whistleblower's claims, including the FBI's corroboration of many of the problems she raised, has been in the public record for more than two years. I appreciated your statement that the retroactive classification order was not intended to place a gag on Congress. However, the notice received by staff members of the Judiciary Committee was very vague, referring only to "some" information conveyed in the briefings. If state secrets are truly implicated by something that was said in an unclassified briefing two years ago, the FBI should provide very specific instructions to current and former staff on what information must be kept secret. Will you instruct your staff to provide more specific information to relevant staff about what, exactly, from the 2002 briefings is classified and what is not?



b5

33. OGC. You testified that, prior to the PATRIOT Act, "if a court-ordered criminal wiretap turned up intelligence information, FBI agents working on the criminal case could not share that information with agents working on the intelligence case." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT, and whether a court could authorize such information-sharing, regardless of any such law or laws?

Response: Prior to the changes brought about by the Patriot Act, Title 18 Section 2517 was interpreted to solely authorize the sharing of intercepted wire, oral, or electronic

~~SECRET~~

~~SECRET~~

communications for criminal law enforcement purposes without the need to obtain a court order. Sharing intercepted information for foreign intelligence purpose required a court order and, based upon the statutory language, it was unclear whether a judge would sign an order. The changes to the Patriot Act clearly allow the sharing of foreign intelligence information developed during a court-ordered criminal wiretap with the agents working intelligence cases.

34. OGC. You further testified that, prior to the PATRIOT Act, "information could not be shared from an intelligence investigation to a criminal investigation." Please state specifically what law or laws prevented such information-sharing prior to PATRIOT?

Response: Prior to the Patriot Act, there were procedures for sharing information between intelligence investigators and criminal agents and prosecutors, but they were difficult, burdensome and usually resulted in less than fulsome sharing. For example, the FISA statute was interpreted to require a "primary purpose" of gathering intelligence in order to secure a FISA Court order. Because of this interpretation of the FISA statute, the Department of Justice and the FISA Court required that certain procedures be followed in order to share intelligence with criminal investigators and prosecutors.

b5

For additional information, see the answer to question 35.

35. OGC. In his statement to the 9/11 Commission, the Attorney General blamed the creation of the so-called "wall" between criminal investigators and intelligence agents on a 1995 memorandum authored by a senior official in the Reno Justice Department, now a member of the 9/11 Commission.

a. Do you agree that the architecture of the wall was in place long before 1995, having its genesis in established legal doctrine dating from 1980? If not, how do you explain the extensive discussion of this issue in the one and only reported opinion of the FISA Court of Review, decided on November 18, 2002?

~~SECRET~~

~~SECRET~~

b5



b5



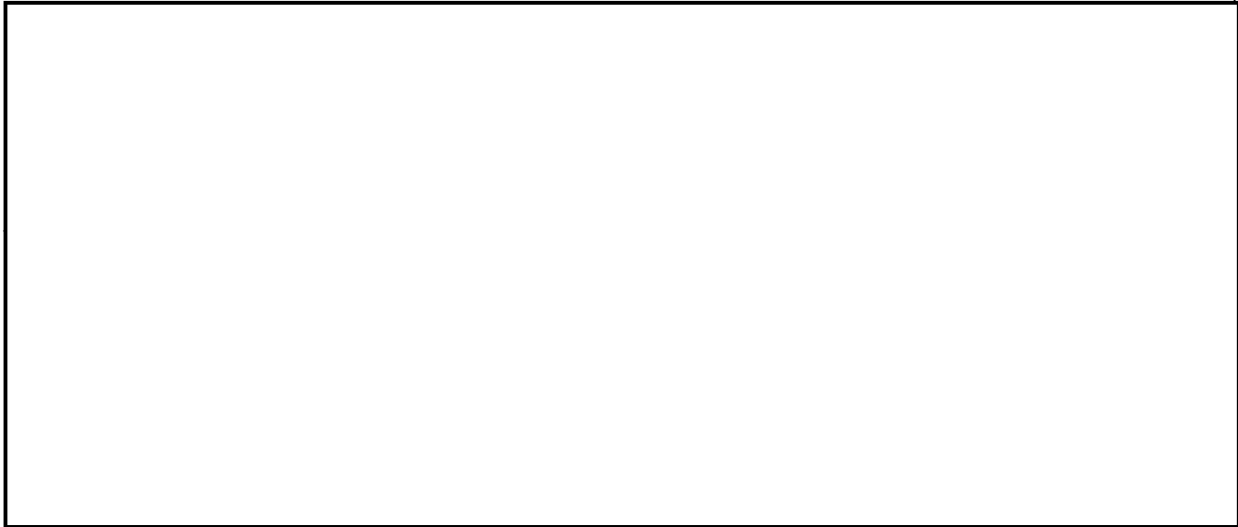
b5



~~SECRET~~

~~SECRET~~

b5



How did the FBI handle information-sharing between criminal investigators and intelligence agents before 1995?

b5



b. Do you agree that the Gorelick memo established proactive guidelines amidst a critically important terrorism prosecution to *facilitate* information sharing..

b5



~~SECRET~~

~~SECRET~~

b5 which account for approximately 75% of the total FISAs for the FBI. The remaining FBI field offices are in the process of being trained on the FISAMS. [REDACTED]

High Performance Technologies, Inc. (HPTi) is the contractor for the development of the FISAMS. During FY 2003, we currently have allocated \$900,000 for Version 1.0 of the FISAMS. We are contracting an additional \$1 million with HPTi for enhancements beginning September 2004, which was funded by the Wartime Supplemental Funds received by the FBI. There will be several follow-up versions to further enhance the FISAMS in the future.

b5 [REDACTED]  
FY06 is the first budget cycle the FISA Unit has been able to formally request funding for this project.

59. OGC. (Follow-up to Leahy 18C) Did you personally review the 4 FISA applications reportedly not approved by the FISA court last year? Can you provide any details on why the 4 applications were not approved?

b5 [REDACTED]

60. OGC. (Follow-up to Leahy 18D) Can you provide us with a blank copy of the FISA Request Form referenced in your response? Will you provide us with a blank copy of the form that the FBI created for requesting business records from the FISA court?

b5 [REDACTED]

~~SECRET~~



~~SECRET~~

b5

61. OGC. (Follow-up to Leahy 21) Did you refer the question to DOJ OIPR? When? Have you been asked to assist in the response? When?

OCA Note: OCA proposes to respond that the FBI forwarded its responses to DOJ on 10/22/03, including our indication that the answer to Senator Leahy's question 21 called for classified information, which is ordinarily supplied to Congress by DOJ's Office of Intelligence Policy and Review (OIPR). By letter to the Committee dated 3/4/04, DOJ's Office of Legislative Affairs forwarded the Department's responses to the Committee, including the FBI's original response to this question.

Response: OGC concurs with OCA's response.

74. CTD. In June 2003, Glenn Fine, the Inspector General for the Justice Department, found "significant problems in the way the detainees were handled" following 9/11. These problems included a failure by the FBI to distinguish between detainees whom it suspected of having a connection to terrorism and detainees with no connection to terrorism; the inhumane treatment of the detainees at a federal detention center in Brooklyn; and the unnecessarily prolonged detention resulting from the Department's "hold until cleared" policy - made worse by the FBI's failure to give sufficient priority to carrying out clearance investigations. In your opinion, has the Justice Department responded in an appropriate manner to all the abuses identified in the Inspector General's report? What steps has the FBI taken to prevent such abuses from occurring in the future?

~~SECRET~~

~~SECRET~~

b5

84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same act makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.

a. OGC. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure for the disclosure of information" as provided for in Section 203. Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

Response to Q84 a: On September 23, 2002, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the Patriot Act. A copy of the guidelines is attached. The Office of the General Counsel issued an EC advising all Divisions of the procedures. A copy of the EC is attached.

b. OGC. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?

Response: This information may be disseminated in any format deemed appropriate for the particular circumstances.

b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203 (b) material?

(1) If so, how many such reports have been

~~SECRET~~

~~SECRET~~

issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

c. OGC. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?

b5

(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?

(1) If so, how many such reports have been issued?

(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

d. OGC. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.

b5

~~SECRET~~

~~SECRET~~

[REDACTED] b5

e. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

f. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: [REDACTED] b5

[REDACTED] OGC strongly believes that Section 203 (b) and (d) should not be allowed to expire on December 31, 2005. The changes brought about by the Patriot Act have significantly increased the ability of the FBI to share information. [Note: DOJ has provided or is in the process of providing examples of how the Patriot Act has been an asset to our investigations and why the sunset provisions should not sunset. We refer OCA to the DOJ for these examples.]

85. Sections 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains to the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

Response:

a. How often has this authority been used, and with what success?

[REDACTED] b5

~~SECRET~~

~~SECRET~~

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response: FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. [REDACTED]

b2

b7E

b5

More specifically, the FBI shares many forms of foreign intelligence with other members of the Intelligence Community, [REDACTED]

b5

[REDACTED] through direct classified and unclassified dissemination and through websites on classified Intelligence Community networks. The FBI also shares intelligence with representatives of other elements of the Intelligence Community who participate in Joint Terrorism Task Forces (JTTFs) in the United States or with whom the FBI collaborates in activities abroad. FBI intelligence products shared with the Intelligence Community include Intelligence Information Reports (IIRs), Intelligence Assessments, and Intelligence Bulletins.

The FBI also disseminates intelligence information through Law Enforcement Online (LEO), a virtual private network that reaches federal, state, and law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes finished FBI intelligence products available, including Intelligence Assessments resulting from analysis of criminal, cyber, and terrorism intelligence. [REDACTED]

b5

[REDACTED] Intelligence Information Reports also are available on LEO at the Law Enforcement Sensitive classification level. The FBI also recently posted the requirements document on LEO, which provided state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.

(i) If so, how many such reports have been issued?

Response: In the past two years the FBI's Counterterrorism

~~SECRET~~

~~SECRET~~

Division's Terrorism Reports and Requirements Section has disseminated 76 intelligence information reports (IIRs) containing information derived from FISA-authorized surveillance and/or search. (Statistics are not maintained in such a way that would enable us to say whether any of the FISA-derived information in the reports was obtained using "roving authority.") Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 electronic information reports containing FISA-derived information.

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: The Office of Intelligence promulgated the FBI's Intelligence Information Report Handbook on 9 July. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The Office of Intelligence is working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with our law enforcement and intelligence community partners, [REDACTED]

b5

In addition, the FBI's Inspection Division has established evaluation criteria for the value of human source reporting, [REDACTED] access and responsiveness to local FBI field office, FBI program and national intelligence requirements. The Office of Intelligence is developing guidelines to use this same criteria as a means of evaluating the value of raw intelligence. Initial discussions on this issue have been held with representatives from the Counterintelligence, Counterterrorism, Criminal and Cyber Divisions. The results of these discussions are being incorporated into evaluation guidelines.

c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

~~SECRET~~

~~SECRET~~

Response: No, the FBI does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, to allow for surveillance against all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the Foreign Intelligence Surveillance Court issue a "generic" secondary order, along with specified orders, for a specifically identified FISA target, that the FBI could serve in the future on the unknown (at the time the order is issued) cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear in a detailed affidavit to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. The roving order has the additional requirement of a judge's approval to monitor more than one telephone. But now, each time a target changes his cellular telephone, instead of going through the lengthy application process, government agents can use the same order to monitor the target. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the Court for a new secondary order. The FBI views this as a vital and necessary tool to counter certain targets who engage in such actions as a deliberate means of evading surveillance.

(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.

Response: The FBI has filed no such briefs on this subject.

d. Inspection Division

e. Based upon the application of this provision of law during

~~SECRET~~

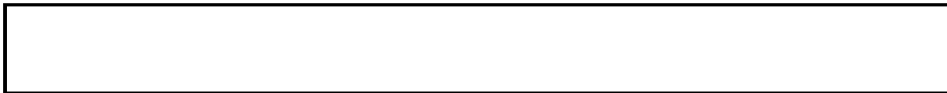
~~SECRET~~

the period since its passage, are there changes to this statute which the Congress should consider?

Response: No, we request only that the provision be preserved.

86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.

a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.



b5

b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate.

Response: None of which the FBI is aware.

c. Inspection Division

d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response: None at this time.

89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.

a. OGC. In how many cases has this authority been used?

~~SECRET~~



~~SECRET~~

b5

(i) How many of such cases were terrorism-related?

b. OGC. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?

Response: OGC does not have a way to determine how many pen registers evolved into full FISA's.

c. Inspection Division. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non-content communications? If such regulations or directives have been issued, please provide copies to the Committee.

d. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

Response: Please see answer to Question 85.

90. Section 215 of the USA-Patriot act authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application

~~SECRET~~

~~SECRET~~

of this provision since its inception.

a. OGC. How many times has this authority been used, and with what success?

b. OGC. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.

c. OGC. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenae are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

d. OGC. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

e. OGC. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?

(i) If so, how many such reports have been issued?

(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?

f. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation

~~SECRET~~

~~SECRET~~

received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

g. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

b1

b7A

b5

Response:

(S)

b5

~~(S)~~

(U)

b5

(U)

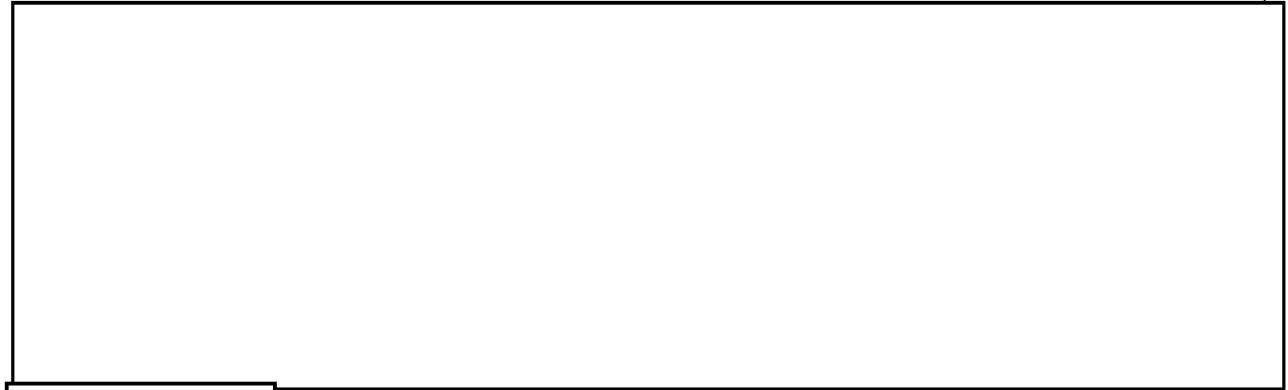
b5

b5

~~SECRET~~

~~SECRET~~

b5



(U)

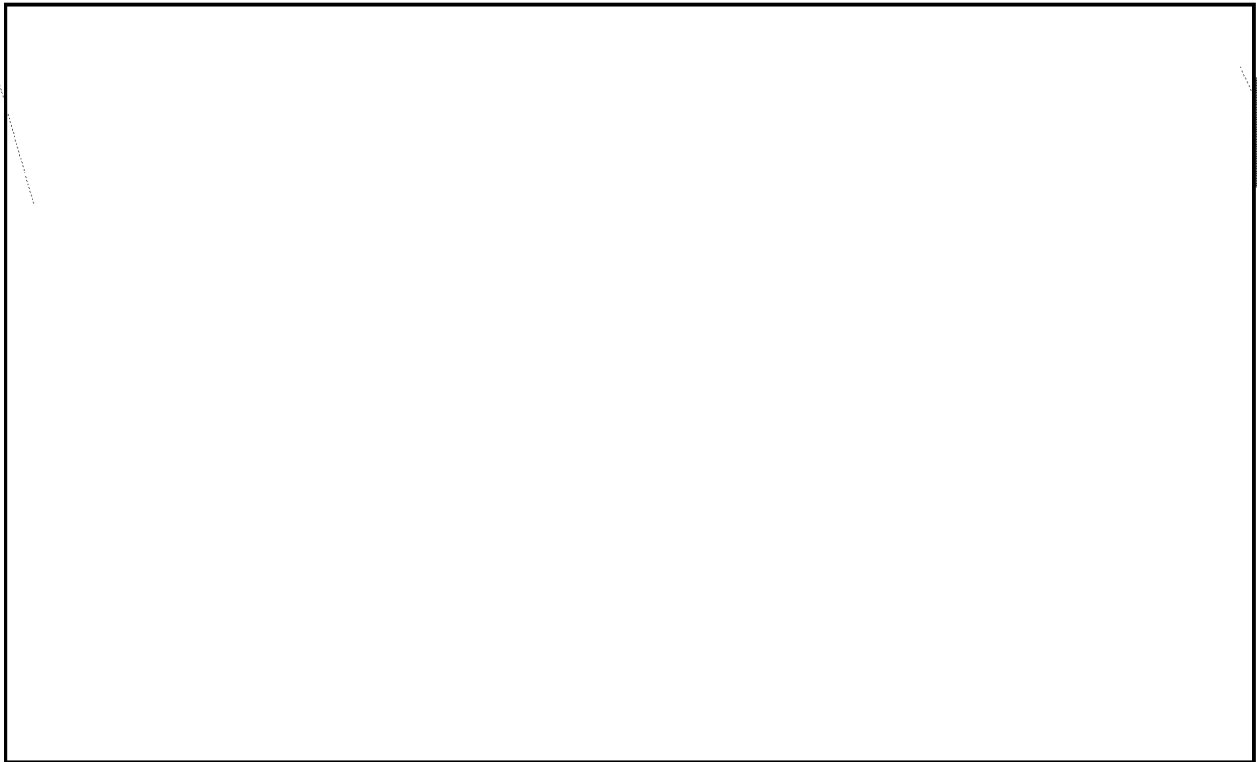


(U)

(S)

b1

b5



(S)  
(S)

b5



~~SECRET~~

~~SECRET~~

b5

b5

b5

92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation

~~SECRET~~

~~SECRET~~

of this provision since its passage.

a. OGC. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."

b. Inspection Division. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

b5

b5

~~SECRET~~

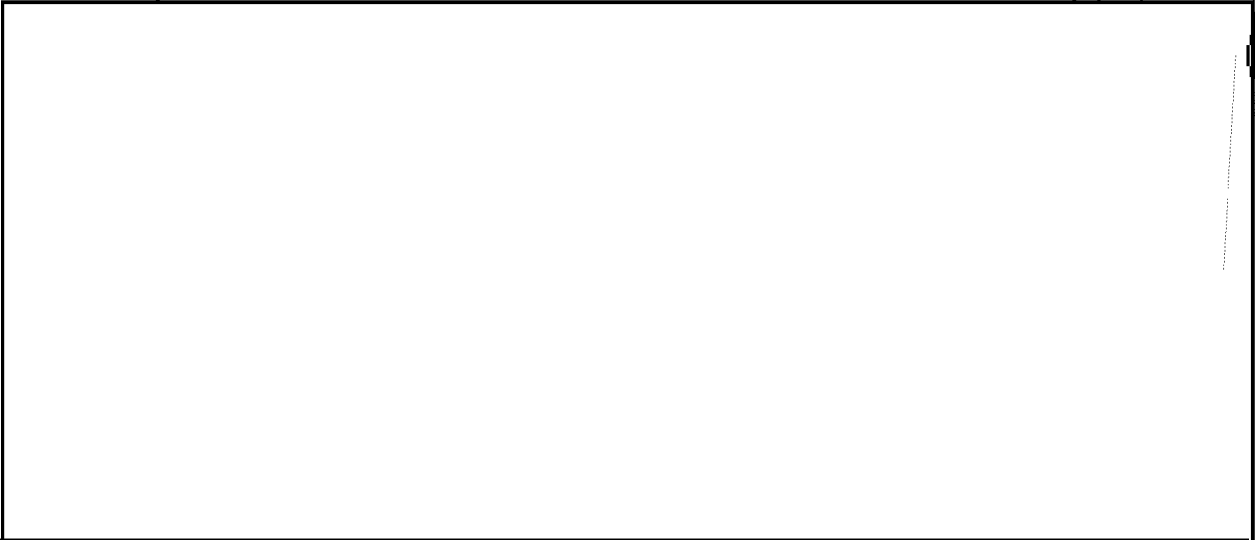
~~SECRET~~

b5



(S)

b1  
b5  
b7A



(S)



(S)



b5  
b6  
b7C



~~SECRET~~

~~SECRET~~

b5  
b6  
b7C  
b7A

b5  
b7A

(S)

(S)

(S)  
(S)

b1  
b5  
b7A

~~SECRET~~



~~SECRET~~

intelligence needs.

b1  
b5  
b7A

(S)  
(S)

b5  
b6  
b7C

c. OGC. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which Congress should consider?

b5

101 d. OGC. According to court records, no criminal charges were ever filed against Mayfield. Instead, he was detained as a material witness. Why was Mayfield held as a material witness and not charged with any criminal conduct?

~~SECRET~~

~~SECRET~~

b5  
b6  
b7C

100 e. CTD (in coordination with OGC). Mayfield has stated that he believes that his home was secretly searched before he was declared a material witness and detained. Prior to, or during his detention, was the Mayfield residence or office searched pursuant to a warrant under the Foreign Intelligence Surveillance Act (FISA) or a delayed notification search warrant? If the latter, please indicate (a) the basis for seeking delayed notice of the search warrant and (b) the time period requested and granted for delaying notice.

b1  
b5  
b6  
b7C

103. OGC. In September 2003, the U.S. Department of Justice disclosed that it had not yet used section 215 of the USA PATRIOT Act. On March 9, 2004, I sent a letter to the Attorney General asking him to clarify whether section 215 has been used since September 18, 2003. (Copy of letter attached.)

a. Please indicate whether section 215 has been used since September 18, 2003.

b. If section 215 has been used, please describe how it has been used. How many U.S. persons and non-U.S. persons were targets of the investigation? Was the section 215 order served on a library, newsroom, or other First Amendment sensitive place? Was the product of the search used in a criminal prosecution?

b1  
b5  
b7A

~~SECRET~~

~~SECRET~~

(S)

b1

b5

b6

b7C

b7A

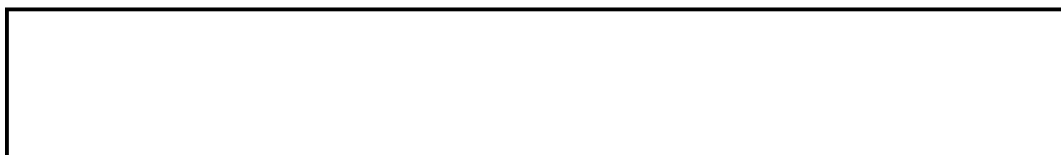
~~SECRET~~

coordination, law enforcement agents and prosecutors learned from intelligence officers that an April 2003 telephone conversation between Dumeisi and a co-conspirator corroborated evidence that Dumeisi was acting as an agent of the Iraqi government, providing a compelling piece of evidence at Dumeisi's trial.

**b. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 218 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.**

**Response:**

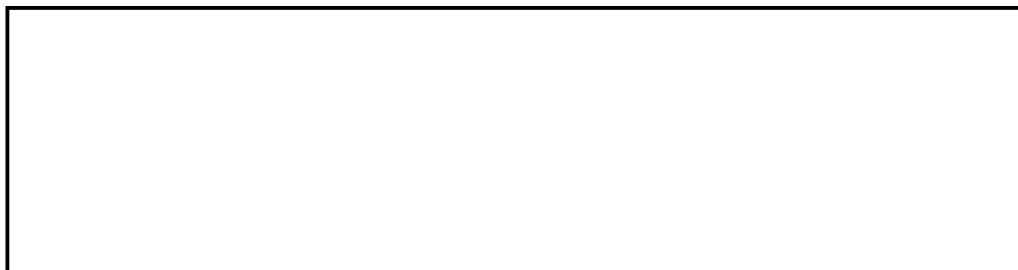
b5

A large rectangular black box used to redact the response to question b.

**c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

b5

A large rectangular black box used to redact the response to question c.

**93. Section 220 of the USA-Patriot Act, "Nationwide Service of Search Warrants for Electronic Evidence" allows for the execution of a search warrant seeking electronic data anywhere in the country. This question pertains to the implementation of this provision since its passage.**

**a. In how many cases has this authority been used?**

**Response:**

While the FBI does not require or maintain centralized statistics on the use of search warrants, Field Offices indicate that they have routinely relied on this

provision (codified at 18 U.S.C. 2703(a)) and can safely estimate that, nationwide, this search authority has been used at least 100 times since its passage.

In section 220 of the USA PATRIOT Act, Congress adapted federal law to changing technology by allowing courts to order the release of stored communications through a search warrant valid in another specified judicial district. The ability to obtain this information with greater efficiency has proven invaluable in numerous cases, including: several terrorism investigations (such as the Virginia Jihad case described above and a complex terrorism financing case in which it was used to obtain a subject's e-mail related to a 7/4/02 shooting at Los Angeles International Airport); child pornography cases in which it is used to obtain information from ISPs regarding those trading sexually exploitive images of children; investigations of "carders" (those who use and trade stolen credit card information); and numerous investigations into Internet sales of counterfeit products, which have led to several indictments and the seizure of bank and financial accounts.

Child pornography cases highlight the benefit of Section 220, because the ability to obtain a search warrant in the jurisdiction of a child pornography investigation rather than in the jurisdiction of the ISP is critical to the success of a complex, multi-jurisdictional child pornography case. In the absence of section 220, law enforcement agents would either have to spend hours briefing other agents across the country so they could obtain warrants in those jurisdictions, or travel hundreds or thousands of miles to present warrant applications to local magistrate judges. Without Section 220, one of two things would often occur in light of limited law enforcement resources: either the scope of the investigation would be narrowed or the case would be deemed impractical at the outset and dropped.

The following case, included in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work," provides an additional example of the benefits afforded by Section 220. A man, armed with a sawed-off shotgun, abducted his estranged wife and sexually assaulted her. Then, after releasing his wife, he fled West Virginia in a stolen car to avoid capture. While in flight, he contacted cooperating individuals by e-mail using an Internet service provider (ISP) located in California. Using the authority provided by section 220, investigators in West Virginia were able to obtain an order from a federal court in West Virginia for the disclosure of information regarding the armed fugitive's e-mail account, including the California ISP. Within a day of the order's issuance, the ISP released information revealing that the fugitive had contacted individuals from a public library in a small town in South Carolina. The very next day, Deputy U.S. Marshals went to the town and noticed a carnival set up next to the public library. Because they were aware that the fugitive had previously worked as a carnival

worker, the Deputy Marshals went to the carnival and discovered the stolen car, arresting the fugitive as he approached the car. He later pled guilty in state court and was sentenced to imprisonment for 30 years. In this case, the fast turn-around on the order for information related to the fugitive's e-mail account, made possible by section 220 of the USA PATRIOT Act, was crucial to his capture.

Section 220 has also made the process of obtaining a warrant for ISP information much more efficient. Before the USA PATRIOT Act, judicial districts that are home to large ISPs were inundated with search warrant requests for electronic evidence. For example, the U.S. Attorney's Office in Alexandria, Virginia, was receiving approximately 10 applications each month from United States Attorney's Offices in other districts for search warrants for the records of an ISP located there. For each of these applications, an Assistant United States Attorney in Virginia and a law enforcement agent in the district had to learn all the details of another district's investigation in order to present an affidavit to the court in support of the search warrant application. Because of section 220, however, these attorneys and Agents can now spend their time on local cases and investigations rather than on learning the details of unrelated investigations being worked through distant offices. Given the short time for which ISPs typically retain records, this provision has enabled the FBI to obtain critical information that may otherwise have been lost or destroyed in the ordinary course of the ISP's business. Section 220 also results in a more efficient use of judicial resources by allowing the judge with jurisdiction over the offense to issue the warrant and retain oversight over the search.

**b. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 220 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.**

**Response:**

b5

**c. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

No. The FBI requests only that the provision be preserved.

The FBI has interviewed Padilla and other enemy combatants. FBI Agents conducting interviews of enemy combatants adhere to the FBI policy governing interviews of persons in the U.S., with the one exception that enemy combatants are not advised of Miranda rights prior to the interrogation.

**b. How many individuals have been arrested or detained pursuant to this authority?**

**c. How many United States citizens have been arrested or detained pursuant to this authority?**

**d. How many United States persons, as defined in Executive Order 12333, Section 3.4(i), and excepting United States citizens, have been arrested or detained pursuant to this authority?**

**Response to b through d:**

Information concerning the designation and detention of enemy combatants is not maintained by the FBI.

**e. What rules, procedures or practices govern the conditions of confinement and the methods of interrogation used in cases where an individual has been arrested or detained pursuant to this authority?**

**Response:**

Rules, procedures, and practices concerning the conditions of confinement and methods of interrogation of enemy combatants by DOD are not maintained by the FBI. When FBI Agents interview enemy combatants or detainees, standard FBI interview policies and practices apply.

**82. Title 18 Section 3103a, as amended by Section 213 of the USA-Patriot Act (P.L. 107-56), provides authority for delaying notice of the execution of search warrants. The following question pertains to the use of the authority provided in this section in investigations or prosecutions related to terrorism during the period of time from September 11, 2001 to the present.**

**a. In how many such cases has the authorities to delay notification been used?**

b. In how many such cases has the authority added by Section 213(b)(1), which allows a delay where "the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result" been used? Please describe the circumstances in each of these cases.

c. In how many such cases has the authority set forth in 18 U.S.C. 2705(E), which provides for delay in cases which would "otherwise seriously jeopardize an investigation or unduly delay a trial" been used? Please describe the circumstances in each of these cases?

Response:

b5

83. Sections 201 and 202 of the USA-Patriot Act added a number of offenses to the "predicate offense list" applicable to criminal wiretaps pursuant to Chapter 119 of Title 18. The following question pertains to the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. In how many cases . . . have the newly-added predicate offenses been used to support an application for a criminal wiretap under the authority of Chapter 119 of Title 18?

Response:

The FBI applied for Title 18 wiretap orders in eight investigations into international terrorism since passage of the USA PATRIOT Act. In only one of those investigations was a newly added terrorism offense used as the sole predicate offense; traditional criminal offenses were used as the predicates for the remaining seven. It cannot be determined, however, whether probable cause as to one or more of the new terrorism predicate offenses was also established, but simply not listed, in those seven cases.

b. In how many such cases has the newly-added predicate offense been the only predicate offense asserted as the basis for the warrant, i.e., where a warrant could not have been lawfully issued but for the passage of the additional criminal predicates?

Response:



In the one case referred to above, the terrorism predicate was the only one asserted. It is not known, however, whether there was probable cause to believe the subjects were engaging in other predicate offenses which were simply not listed, or whether there was probable cause only with respect to the terrorism offense.

**c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Sections 201 or 202 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.**

Response:

b5

**d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute, including the addition of predicate crimes, which the Congress should consider?**

Response:

Sections 201 and 202 of the USA PATRIOT Act are currently scheduled to expire at the end of 2005. The FBI strongly supports making these important statutory provisions permanent. In addition, the FBI would ask Congress to consider amending 18 U.S.C. 2516 to allow for the use of existing electronic surveillance authorities in investigating the full-range of terrorism related crimes. In particular, Congress should consider adding the following predicate offenses to those currently listed in 18 U.S.C. 2516(1): 1) 18 U.S.C. 37 (relating to violence at international airports); 2) 18 U.S.C. 930(c) (relating to an attack on a federal facility with a firearm); 3) 18 U.S.C. 956 (conspiracy to harm persons or property overseas); 4) 18 U.S.C. 1993 (relating to mass transportation systems); 5) an offense involved in or related to domestic or international terrorism as defined in 18 U.S.C. 2331; 6) an offense listed in 18 U.S.C. 2332b(g)(5)(B); and 7) 18 U.S.C. 2332d.

While the few statistics listed in response to questions 83 a and b, above, may be understood to indicate limited use of this new authority and limited value of these new USA PATRIOT Act sections, this would not be correct. In most international terrorism investigations since October 2001, electronic surveillance

has been successfully pursued under FISA authority and, therefore, the criminal terrorism predicates under Title 18 were not necessary. Nevertheless, in future investigations in which probable cause regarding connection to a foreign power cannot be as easily established (and thus FISA surveillance is not an option); these new USA PATRIOT Act provisions will permit the use of a federal wiretap in response to significant terrorist threats. The flexibility to use either foreign intelligence collection tools or criminal evidence gathering processes, and to share the results, is an important feature of the USA PATRIOT Act in the war against terrorism.

**84. Sections 203(b) and 203(d) of the USA-Patriot Act provide specific authority for the provision of intelligence information acquired in the course of a criminal investigation to elements of the Intelligence Community. Section 901 of the same [A]ct makes such disclosure in most cases mandatory. The following questions pertain to the implementation of these sections.**

**a. Section 203(c) of the USA-Patriot Act requires the Attorney General to "establish procedures for the disclosure of information" as provided for in Section 203. Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.**

**Response:**

On 9/23/02, the Attorney General promulgated guidelines that established the procedures for disclosure of information under Section 203 of the USA PATRIOT Act. Those guidelines, and the FBI's instructions to the field with respect to those guidelines, follow.

**b. Section 203(b) specifically provides authority "to share electronic, wire, and oral interception information" where such information is foreign intelligence information. What is the method for disseminating such information to the Intelligence Community?**

**Response:**

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the USIC through any means appropriate to the circumstances, including Intelligence Information Reports (IIRs), Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

**(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(b) material?**

**Response:**

The FBI disseminates intelligence information via the IIR, which is an electronic communication format widely accepted in the USIC as the standard intelligence dissemination vehicle. IIRs consist of raw intelligence (intelligence which has not been finally evaluated) and associated clarifying information that puts the raw intelligence into context. IIRs are drafted and prepared by the FBI's cadre of Intelligence Analysts/Reports Officers. Before FBI intelligence is disseminated, it is analyzed and sanitized to protect intelligence sources and methods and, if applicable, United States persons and entities that may be compromised or negatively impacted if left unprotected. FBI Program Managers and Intelligence Analysts concurrently identify intelligence that is consistent with USIC intelligence requirements and interests.

**(1) If so, how many such reports have been issued?**

**Response:**

Although CTD is not the only FBI producer of IIRs, that Division reports that, during the period from August 2002 (when statistical data was first collected) through August 2004, CTD has disseminated approximately 3,860 IIRs, 240 of

which have contained FISA-derived intelligence. The remaining IIRs have been derived from various sources and methods which may or may not include Title III information.

The FBI does not track or maintain a central database with respect to the number of IIRs containing 203(b) material, if any.

**(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?**

**Response:**

Determinations to disseminate electronic, wire, and oral intercept information are made with input from Operational Program Managers, Intelligence Analysts, the National Security Law Branch, and, when appropriate, DOJ. This evaluation considers the value of the information not only to the USIC but also, depending on the proposed use, context, and nature of any threat-related information, to federal, state, and local law enforcement entities and, when authorized by DOJ, to foreign intelligence services and foreign law enforcement agencies.

The quality and value of IIRs are evaluated through several means. On each IIR, the Reports Officer provides information by which the customers can contact the Reports Officer directly. The quality and relevance of the reporting is also reflected by the submission of additional collection requirements; USIC members often forward formal Requests for Information (RFIs) with respect to information that has been protected (not provided) in the IIR, such as U.S. Person information. Such RFIs provide an excellent indication of USIC interest in FBI reporting. In addition, USIC members often provide feedback with respect to specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. The FBI's OI also often receives evaluations of FBI reporting, and is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

**c. Section 203(d), the so-called "catch-all" provision, provides a general authority to share foreign intelligence information with the Intelligence Community. What is the method for disseminating such information to the Intelligence Community?**

**Response:**

The FBI shares foreign intelligence information, as defined in Section 203(d)(2), with the USIC through several conduits. Dissemination can be through direct classified and unclassified IIRs, Intelligence Assessments, Intelligence Bulletins, Teletype Memoranda, or USIC web sites on classified networks. The FBI also shares intelligence information through the FBI's Joint Terrorism Task Forces (JTTFs), which include members of the USIC and operate in 84 locations across the United States. Unclassified but "law enforcement sensitive" intelligence information is also disseminated to federal, state, and local law enforcement intelligence components through Law Enforcement Online (LEO), a computer network which provides finished intelligence products, assessments, and bulletins on significant developments and trends.

**(i) In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of Section 203(d) material?**

**Response:**

Electronic, wire, and oral interception information derived through standard criminal procedures may be disseminated to the USIC through any appropriate means, including IIRs, Teletype Memoranda, Intelligence Assessments, Intelligence Bulletins, and FBI Letterhead Memoranda.

**(1) If so, how many such reports have been issued?**

**Response:**

While the FBI does not track or maintain a central database with respect to the number of IIRs containing 203(d) material, if any, the July 2004 DOJ "Report From the Field: The USA PATRIOT Act at Work" indicates that DOJ has made disclosures of vital information to the intelligence community and other federal officials under section 203 on many occasions. For instance, such disclosures have been used to support the revocation of visas of suspected terrorists and prevent their reentry into the United States, to track terrorists' funding sources, and to identify terrorist operatives overseas.

**(2) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?**

**Response:**

There are various means by which IIRs are evaluated. Members of the USIC often provide feedback assessing the quality and value of specific IIRs directly to the FBI Intelligence Analysts/Reports Officers who author the reports. On each IIR, the Reports Officers identify the means by which customers can contact them directly. IC members assess the quality and relevance of the reporting, and submit additional collection requirements when appropriate. Often, IC members forward formal Requests for Information (RFIs), which can provide an excellent indication of IC interest in FBI reporting. The FBI's OI also receives evaluations of FBI reporting. The OI is working to establish a formal IIR evaluation mechanism by which recipients can rate or provide feedback on FBI intelligence reporting.

**d. Section 905(c) of the USA-Patriot Act requires the Attorney General to "develop procedures for the administration of this section. . . ." Have such procedures been promulgated? If so, please provide a copy of those procedures to the Committee.**

**Response:**

b5

**e. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 203 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.**

**Response:**

b5

**f. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

b5

b5

85. Section[ ] 206 of the USA-Patriot Act, the so-called "roving wiretap" provision, permits the issuance of a FISA warrant in cases where the subject will use multiple communication facilities. This question pertains [to] the implementation of this section during the time period since the passage of the USA-Patriot Act, October 26, 2001.

a. How often has this authority been used, and with what success?

Response:

b5

b. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to the FISA?

Response:

FBI intelligence products are an important vehicle for the dissemination of both FISA-derived and non-FISA foreign intelligence information, but not the only one. The FBI shares many forms of foreign intelligence with other members of the USIC through direct classified and unclassified disseminations, through web sites on classified USIC networks, through its participation in Joint Terrorism Task Forces (JTTFs), and through its collaboration in activities abroad.

FBI intelligence products shared with the USIC include IIRs, Intelligence Assessments, and Intelligence Bulletins. The FBI also disseminates intelligence information through LEO, a virtual private network that reaches federal, state, and local law enforcement agencies at the Sensitive But Unclassified (SBU) level. LEO makes available to all users finished FBI intelligence products, including intelligence assessments resulting from the analysis of criminal, cyber, and terrorism intelligence, finished intelligence concerning significant developments or trends, and IIRs that are available at the SBU level. In addition, the FBI

recently posted the requirements document on LEO, providing to state and local law enforcement a shared view of the terrorist threat and the information needed in every priority area.

**(i) If so, how many such reports have been issued?**

**Response:**

In the past two years, CTD's Terrorism Reports and Requirements Section has disseminated 76 IIRS containing information derived from FISA-authorized surveillance and/or searches. (Statistics are not maintained in a way that would enable us to advise whether any of the FISA-derived information in the reports was obtained using roving wiretap authority.) Other FBI Divisions have also issued reports containing FISA-derived information. For example, the Cyber Division has written a total of 24 IIRs containing FISA-derived information.

**(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?**

**Response:**

The OI promulgated the FBI's Intelligence Information Report Handbook on 7/9/04. The Handbook establishes the first comprehensive FBI-wide guide for the format and content of raw intelligence reports. The OI is also working to develop evaluation guidelines based, in part, on the criteria established in the Handbook for the types of information to be reported and shared with law enforcement and USIC partners.

In addition, the FBI's Inspection Division has established criteria for assessing: the value of human source reporting; access to and the responsiveness of local FBI field offices; and FBI program and national intelligence requirements. The OI is developing guidelines according to which it will use these same criteria as a means of assessing the value of raw intelligence. Initial discussions on this issue have been held with the CI, CT, Criminal, and Cyber Divisions, and the results of these discussions are being incorporated into evaluation guidelines.

**c. Some have read this section as providing for surveillance in cases where neither the identity of the subject or the facility to be used is known -- in effect, allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept conversation of an unknown person. Is this the reading of the statute being**



adopted by the Federal Bureau of Investigation and the Department of Justice? If not, please provide your interpretation of this authority.

**Response:**

No, the FBI does not interpret the statute as allowing for the authorization of FISA surveillance against all phones in a particular geographic area to try to intercept the conversations of an unknown person. In order to make a showing of probable cause, the FISA statute requires a statement of the facts and circumstances relied upon by the applicant for surveillance to justify the belief that: (1) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and, (2) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power. Thus, the FISA statute does not permit coverage to be authorized, with or without the "roving wiretap" provision, for surveillance of all persons in a particular geographic area. The FBI has interpreted the "roving" authority as permitting the FBI to request that the FISA Court issue, along with the primary order, a "generic" secondary order with respect to a specifically identified FISA target that the FBI can serve in the future on a currently unknown cell phone carrier, Internet service provider, or other communications provider, if the target rapidly switches from one provider to another. The roving wiretap order still requires that a federal law enforcement agent swear, in a detailed affidavit, to facts establishing probable cause, and still requires a court to make a finding of probable cause before issuing the order. While the roving order carries the additional requirement of a judge's approval to monitor more than one telephone, it permits government agents to continue to monitor the target, even if the target changes to a different cellular telephone, rather than first going through the lengthy application process to monitor that new phone. This will allow the FBI to go directly to the new carrier and establish surveillance on the authorized target without having to return to the FISA Court for a new secondary order. The FBI views this as a vital tool to counter targets who change cell phone providers or other communication channels as a deliberate means of evading surveillance.

**(i) Have any briefs been filed with the Foreign Intelligence Surveillance Court on this subject? If so, please provide copies of such briefs to the Committee.**

**Response:**

The FBI has filed no such briefs on this subject.

**d. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 206 of the USA-Patriot Act? If so, please describe the nature and disposition of such a complaint.**

**Response:**

b5

**e. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

No. The FBI requests only that the provision be preserved.

**86. Section 207 of the USA-Patriot Act extends the time limits provided in the FISA which govern surveillance against agents of a foreign power.**

**a. Has the Federal Bureau of Investigation or the Department of Justice conducted any review to determine whether, and if so, how many, personnel resources have been saved by this provision? If so, please provide the results to the Committee.**

**Response:**

b5

**b. Have there been any cases where, after the passage of the now-extended deadlines it was determined, either by the Department of Justice, the Federal Bureau of Investigation or the Foreign Intelligence Surveillance Court, that surveillance should have been terminated at an earlier point because of the absence of a legally required predicate?**

**Response:**

None of which the FBI is aware.

c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 207 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.

Response:

b5



d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?

Response:

None at this time.

87. Section 209 of the USA-Patriot Act clarified the law with regarding the applicability of criminal search warrants to voice mail. This question pertains to application of this provision since its passage.

a. How many such search warrants have been issued since passage of this act?

Response:

The FBI does not collect or maintain statistics concerning the types of search warrants issued in FBI investigations, including those seeking access to voice mail. Because federal search warrants are requested by U.S. Attorneys' Offices and issued by U.S. District Courts, these statistics may be maintained by one or both of those offices.

b. In such cases, have there been any instances in which a wiretap, as opposed to a search[ ] warrant[, ] would not have been supported by the facts asserted in support of the search warrant.

Response:

This information is unavailable, as indicated above. It is clear, however, that the support needed for a federal wiretap is considerably greater than that required for a search warrant.

**c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 209 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.**

**Response:**

A private citizen who has lodged numerous complaints against the FBI, all of which have been determined to be unfounded pursuant to appropriate inquiry, complained that she was a former FBI employee whose home, vehicles, telephone, and internet had been subject to "aggressive surveillance" since August 2000. FBI investigation revealed that the complainant was, in fact, not a former FBI employee and that the FBI had conducted no surveillance of her for any reason. Based on these findings, this matter was closed by the FBI in July 2003. The FBI has construed this as a complaint with respect to both Section 209 and 217 of the USA PATRIOT Act.

**d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

The FBI is not aware of any substantive changes to this provision warranting Congressional consideration. Section 209 is, however, currently scheduled to expire at the end of 2005, and the FBI strongly supports making this provision permanent. Section 209 allows investigators to use court-ordered search warrants to obtain voice-mail messages held by a third party provider when supported by probable cause. Previously, the Electronic Communications Privacy Act (ECPA), 18 U.S.C. 2703, allowed law enforcement authorities to use search warrants to gain access to stored electronic communications such as e-mail, but not stored wire communications such as voice-mail. Instead, the wiretap statute, 18 U.S.C. 2510(1), governed access to stored wire communications, requiring law enforcement officers to use wiretap orders to gain access to unopened voice-mail. This resulted in voice-mail messages being treated differently than e-mail messages. Voice-mail messages are also treated differently than answering machine messages inside a home, access to which requires a search warrant, because answering machine messages are not regulated under the wiretap statute. Section 209 of the USA PATRIOT Act eliminates the disparate treatment of

similar information. If this section is sunsetted, voice-mail messages will again be treated in a different manner than answering machine messages and stored e-mail information beginning in 2006.

**88. Section 212 of the USA-Patriot Act permits communications service providers to provide customer records or the content of customer communications to the FBI in an emergency situation. This question pertains to application of this provision since its passage, and to all instances, not only to terrorism investigations.**

**a. In how many cases has this provision been used? Please provide a short description of each such case to the Committee.**

**Response:**

Service providers have voluntarily provided information on at least 141 occasions under this provision. Such disclosures have often included both e-mail content and associated records. Several of these disclosures have directly supported terrorism cases under the emergency of a possible pending attack. For example, this provision has been used to obtain access to e-mail accounts used by terrorist groups to discuss various terrorist attacks. It has also been used to respond quickly to bomb and death threats, as well as in an investigation into a threat to a high ranking foreign official. This provision has additionally been used to locate kidnaping victims and to protect children in child exploitation cases. In one kidnaping case involving the abduction of a 14-year-old girl, reliance on this provision allowed the FBI to quickly locate and rescue the child and to identify and arrest the perpetrator. Because of this provision, additional harm to the girl was prevented and she was returned to her family in a matter of hours.

Because many international service providers are located within the United States (such as Hotmail and AOL), Legal Attachés have used this provision to assist foreign law enforcement officials with similar emergencies, such as death threats on prosecutors and other foreign officials. Where time is of the essence, giving service providers the option of revealing this information without a court order or grand jury subpoena is crucial to receiving the information quickly and preventing loss of life or serious injury.

Additional examples are provided in DOJ's July 2004 "Report from the Field: The USA PATRIOT Act at Work."

**b. In any such case have there been any cases in which, except for the time constraints imposed by the emergency situation, a conventional wiretap or search warrant,**

would not have been supported by the facts available to the Government at the time of the emergency request? If so, please describe such situations.

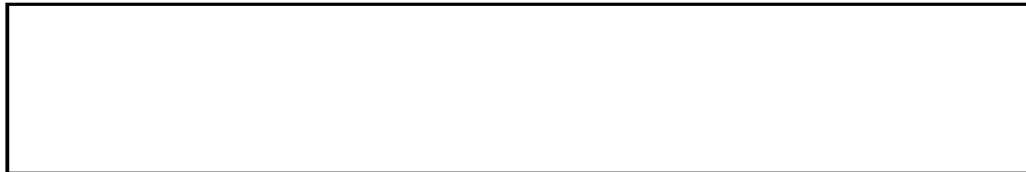
**Response:**

We are aware of no such circumstances. However, it is important to recognize that the information that may be disclosed under this emergency authority is limited to the contents of communications that are in electronic storage and records associated with customers or subscribers. Given this limitation, a conventional wiretap would generally not apply, and a search warrant would be required only for the contents of communications that are held for less than 180 days. Emergency authority is appropriate for the disclosure of information held by a third party and, to the extent the information is constitutionally protected, disclosure of the information under exigent circumstances is entirely consistent with the emergency exception to the warrant requirement of the Fourth Amendment.

**c. Has the Department of Justice or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 212 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.**

**Response:**

b5



**d. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

There is currently a discrepancy between the emergency provisions applicable to contents and records that appears illogical and unjustified. Currently a provider is arguably required under 18 U.S.C. 2702(c)(4) to meet a higher burden for disclosing a record or other subscriber information than is required by § 2702(b)(7) for divulging the contents of a communication in electronic storage. Moreover, the entities to whom a provider may disclose are significantly more restricted for records than for content. The language in (b)(7) was enacted by Pub. L. 107-296 as part of the Homeland Security Act of 2002, with the objective that

all entities with responsibility for ensuring our domestic security would have access to this information in an emergency. It does not appear that the discrepancies between the disclosure of content and records are supported by differing privacy interests inherent in the respective information or by other factors. Accordingly, reconciling these provisions would be appropriate.

**89. Section 214 of the USA-Patriot Act permits the use of FISA pen register/trap & trace orders with respect to electronic communications, and eliminates the requirement that such use be only in the context of a terrorist or espionage investigation. This question pertains to application of this provision since its passage, and to all instances, not only terrorism investigations.**

**a. In how many cases has this authority been used?**

**(i) How many of such cases were terrorism-related?**

**Response to a and a(i):**

The FBI does not maintain this information. It is, instead, maintained by DOJ's OIPR, to whom the FBI defers for response.

**b. Of the cases in which such authority was used, in how many was a subsequent application for a full surveillance order made pursuant to the FISA, or Chapter 19 of Title 18?**

**Response:**

The FBI does not track the number of pen registers that evolve into full FISA's.

**c. Has the Intelligence Community, Department of Justice, or Federal Bureau of Investigation developed regulations or directives defining the meaning of non-content communications? If such regulations or directives have been issued, please provide copies to the Committee.**

**Response:**

The FBI has not developed any such regulations or directives, nor is it aware that the USIC or DOJ have issued guidance defining "non-content communications" in relation to the use of FISA pen register/trap and trace authorities.

**d. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?**

**Response:**

See response to Question 85b, above.

**(i) If so, how many such reports have been issued?**

**Response:**

See response to Question 85b(i), above.

**(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?**

**Response:**

See response to Question 85b(ii), above.

**90. Section 215 of the USA-Patriot [A]ct authorizes the Foreign Intelligence Surveillance Court to issue orders permitting FBI to access "tangible" items in the course of a terrorism or espionage investigation. The following questions pertain to the application of this provision since its inception.**

**a. How many times has this authority been used, and with what success?**

**b. Has this provision been used to require the provision of information from a library or bookstore? If so, please describe how many times, and in what circumstances.**

**Response to a and b:**

b5



c. In your testimony you compared this provision with existing authority in the criminal context, noting that records such as library records are subject to a grand jury subpoena. However, in criminal cases the propriety and lawfulness of subpoenae are to some extent tested in the adversary process of a trial - how, in the context of the FISA, does such a check occur?

**Response:**

The checks on the use of the business record provision are numerous. First, requests for such orders must be approved by several authorities within the FBI and DOJ to ensure they comply with FISA requirements. In addition, however, business record requests must be approved by a FISA Court judge. FISA judges are part of an independent judiciary, appointed pursuant to Article III of the U.S. Constitution.

Business record orders require a showing that the record is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. "Authorized investigations" may only be initiated when consistent with Attorney General guidelines, so the existence of such an investigation and the relevance of the record to this investigation represent two "checks" on this authority. Under both the Attorney General guidelines and section 215 of the USA PATRIOT Act, such investigations may not be premised solely upon the exercise of constitutionally protected activities.

Once an appropriate FBI authority determines that a business record order request is relevant to a properly authorized investigation, the request itself requires numerous layers of approval (as do requests for electronic surveillance, physical search, and pen register/trap and trace orders under FISA). At the FBI field level, such requests must be approved by the Supervisory Special Agent (SSA), the SAC or appropriate Assistant SAC, and the Chief Division Counsel. At the FBIHQ level, the request must be approved by an attorney in the National Security Law Branch, and signed by one of the several designated high-ranking FBI officials to whom certification authority has been delegated. Thereafter, the request is submitted to DOJ's OIPR, and must be approved by OIPR before it is presented to the FISA Court. When presented to the FISA Court, the FISA judge must determine that the request meets FISA requirements before issuing the order.

Lastly, section 215 imposes Congressional oversight by requiring the Attorney General to report to Congress annually on the FBI's use of the section.

d. As of October 2004 the Department of Justice advised that this provision had not been used. If that is true, is there a necessity to maintain this provision in law? Why?

Response:

b5

(i) With respect to the potential applicability of this section to libraries and bookstores, there has been some concern that the mere prospect of use of the statute has a "chilling effect" on the use of these facilities. Can this chilling effect be minimized, if not eliminated, by incorporating a higher threshold for use in the limited context of libraries and bookstores? If not, why not?

Response:

In the context of this question, the FBI can initiate investigations of individuals or groups only under specific conditions articulated in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG). Additionally, FBI guidelines place strict limits on the types of investigative activities that can be undertaken when investigations are opened, requiring, for example, that no investigation of a U.S. person may be conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Individuals' rights are additionally safeguarded by other authorities, such as Executive Order (E.O.) 12333, which is the primary authority for intelligence activities conducted by the USIC. E.O. 12333 establishes goals for the collection of intelligence information; assigns responsibilities among the various intelligence components; prescribes what information may be collected, retained, and disseminated; and prescribes or proscribes the use of specified techniques in the collection of intelligence information. As noted above, the NSIG establishes limits and requirements governing FBI international terrorism investigations with respect to foreign intelligence, CI, and intelligence support activities. Another important internal safeguard is the Intelligence Oversight Board (IOB), which reviews the FBI's practices and procedures relating to foreign intelligence and foreign CI, requiring the FBI to report violations of foreign CI or other guidelines designed in full or in part to ensure the protection of the individual rights of a U.S. person.

**e. In your testimony you made reference to newly-created procedures by which the Federal Bureau of Investigation disseminates intelligence via "electronic intelligence reports" - is this the mechanism used for dissemination of material acquired pursuant to this section of the FISA?**

**Response:**

The IIR is the mechanism by which the FBI disseminates raw intelligence information to the Intelligence, Defense, and law enforcement communities. The intelligence information contained in these IIRs is information generally derived from FBI operations, investigations, or sources. Intelligence information acquired pursuant to Section 215 of the USA PATRIOT Act could be disseminated via an IIR in appropriate circumstances. Between August 2002 and August 2004, the FBI has disseminated approximately 3,860 terrorism-related IIRs.

**(i) If so, how many such reports have been issued?**

**Response:**

None of the information contained in the 3,860 terrorism-related IIRs disseminated between August 2002 and August 2004 was acquired pursuant to section 215 of the USA PATRIOT Act.

**(ii) Has the Federal Bureau of Investigation developed procedures to ascertain the quality and value of such intelligence reports?**

**Response:**

Although the FBI has procedures to evaluate the quality of intelligence reports, no reports have been disseminated which contained information acquired pursuant to section 215 of the USA PATRIOT Act.

**f. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 215 of the USA-Patriot Act? If so, please describe the nature and disposition of any such complaint.**

**Response:**

**g. Based upon the application of this provision of law during the period since its passage, are there changes to this statute which the Congress should consider?**

**Response:**

The FBI has identified no need for change at this time.

**91. Section 217 of the USA-Patriot Act authorizes, without court order, the interception of communications to and from a trespasser with a protected computer. This question pertains to the implementation of this provision since its passage.**

**a. How many times has the authority under this section been used, and with what success? Please provide descriptions of the circumstances where it has been used.**

**Response:**

While the FBI does not maintain statistics on the frequency with which the trespasser authority has been used, we can provide examples of some such cases.

Under this provision, the FBI was able to monitor the communications of an international group of "carders" (individuals who use and trade stolen credit card information). This group used chat rooms and fraudulent web sites, creating false identities to obtain e-mail accounts and then transmitting their communications through a computer that had been "hacked" and set up to operate as their proxy server. A proxy server changes an Internet user's original Internet protocol (IP) address to that of the proxy server so that only the proxy server knows the true point of origin. The owner of the hacked computer was not aware that it was being used as a proxy server, and considered all individuals using the system as a proxy server to be trespassers. The owner provided the FBI with consent to monitor the communication ports solely used by the trespassers, and this monitoring led to the subject's true identity. The subject was indicted in September 2003. Without this authority to monitor, the real identities of the trespassers could easily have remained anonymous.

In another example, a former employee was suspected of illegally accessing a company's e-mail system to gain inside information regarding company concepts

and client information, as well as privileged information regarding legal proceedings between the company and the former employee. The computer intruder used a variety of means to access the system, including wireless modems in laptops and hand-held Blackberry devices, making it more difficult to identify the intruder and to link the computer intrusions to the former employee. The victim company authorized the FBI to monitor the intruder's communications with and through its computer systems.

In another case, a computer-intruder obtained control of a school's network and reconfigured it to establish additional IP addresses that were separate and distinct from those used by the school. This allowed hackers, and others using the Internet who did not want to be located, to jump through the school's system before committing their illegal acts. Monitoring accomplished pursuant to the school's consent resulted in the FBI's identification of over 200,000 different IP addresses using the school system as a proxy to further illegal activity such as fraud, computer intrusions, and spamming.

As these cases make clear, this authority is critical not only to the FBI's ability to identify criminals who engage in computer intrusions but also its ability to identify and investigate additional criminal activities conducted through victims' computers.

**b. Section 217(2)(I) requires authorization by the owner of the computer before the section can be applied. Can this authorization be withdrawn or limited by the owner of the computer? If so, how and in what circumstances?**

**Response:**

Yes. As with any form of consent, which must be freely and voluntarily given to be valid, the consenting party has the right to terminate the consent at any time. The FBI encourages the use of a written consent form containing an express acknowledgment by the consenting owner or operator that states: "I understand my right to refuse authorization for interception and have accordingly given this authorization freely and voluntarily."

**c. Has the Department of Justice, the Director of Central Intelligence (in his capacity as head of the Intelligence Community) or the Federal Bureau of Investigation received any complaints regarding the application or implementation of Section 217 of the USA-Patriot Act? If so, please describe the nature and disposition of each such complaint.**

**Response:**

See response to Question 87c, above.

**92. Section 218 of the USA-Patriot Act created the so-called "significant purpose" test for applications pursuant the FISA, clarifying the law to recognize that in many cases such surveillance may implicate both a law enforcement and an intelligence interest. This question pertains to the implementation of this provision since its passage.**

**a. Please provide the Committee with specific examples, in unclassified form if possible, of cases in which both law enforcement and intelligence interests were "significant."**

**Response:**

As indicated in the July 2004 DOJ publication entitled, "Report from the Field: The USA PATRIOT Act at Work," the removal of the "wall" played a crucial role in the Department's successful dismantling of a Portland, Oregon, terror cell, popularly known as the "Portland Seven." Members of this terror cell had attempted to travel to Afghanistan in 2001 and 2002 to take up arms with the Taliban and al Qaeda against United States and coalition forces fighting there. Law enforcement agents investigating that case learned through an undercover informant that, before the plan to go to Afghanistan was formulated, at least one member of the cell, Jeffrey Battle, had contemplated attacking Jewish schools or synagogues, and had even been casing such buildings to select a target for such an attack. By the time investigators received this information from the undercover informant, they suspected that a number of others were involved in the Afghanistan conspiracy. While several of these other individuals had returned to the United States from their unsuccessful attempts to reach Afghanistan, investigators did not yet have sufficient evidence to arrest them. Before the USA PATRIOT Act, prosecutors would have faced a dilemma in deciding whether to arrest Battle immediately. If prosecutors had failed to act, lives could have been lost through a domestic terrorist attack; if prosecutors had arrested Battle in order to prevent a potential attack, the other suspects in the investigation would undoubtedly have scattered or attempted to cover up their crimes. Because of sections 218 and 504 of the USA PATRIOT Act, however, FBI agents could conduct FISA surveillance of Battle to detect whether he had received orders from an international terrorist group to reinstate the domestic attack plan on Jewish targets, and could keep prosecutors informed as to what they were learning. This gave prosecutors the confidence not to arrest Battle prematurely, but instead to continue to gather evidence on the other cell members. Ultimately, prosecutors were able to collect sufficient evidence to charge seven defendants and then to secure convictions and prison sentences ranging from three to eighteen years for the six defendants taken into custody. Charges against the seventh defendant were

dismissed after he was killed in Pakistan by Pakistani troops on 10/3/03. [REDACTED]

b5 [REDACTED]

DOJ shared information pursuant to sections 218 and 504 before indicting Sami al-Arian and several co-conspirators on charges related to their involvement with the Palestinian Islamic Jihad (PIJ). PIJ is alleged to be one of the world's most violent terrorist organizations, responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom. The indictment states that al-Arian served as the secretary of the PIJ's governing council ("Shura Council"). He was also identified as the senior North American representative of the PIJ. Sections 218 and 504 of the USA PATRIOT Act enabled prosecutors to consider all evidence against al-Arian and his co-conspirators, including evidence obtained pursuant to FISA that provided the necessary factual support for the criminal case. By considering the intelligence and law enforcement information together, prosecutors were able to create a complete history for the case and put each piece of evidence in its proper context. This comprehensive approach was essential to prosecutors' ability to build their case and pursue the proper charges. [REDACTED]

b5 [REDACTED]

Prosecutors and investigators also used information shared pursuant to sections 218 and 504 of the USA PATRIOT Act in investigating the defendants in the so-called "Virginia Jihad" case. This prosecution involved members of the Dar al-Arqam Islamic Center, some of whom trained for jihad in Northern Virginia by participating in paintball and paramilitary training or traveled to terrorist training camps in Pakistan or Afghanistan between 1999 and 2001. These individuals are associates of a violent Islamic extremist group known as Lashkar-e-Taiba (LET), which primarily operates in Pakistan and Kashmir and has ties to the al Qaeda terrorist network. As the result of an investigation that included the use of information obtained through FISA, prosecutors were able to bring charges against several individuals. Nine of these defendants have received sentences ranging from four years to life imprisonment (six were pursuant to guilty pleas and three were contrary to their pleas; charges have included conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban).

Information sharing between intelligence and law enforcement personnel made possible by sections 218 and 504 of the USA PATRIOT Act was also pivotal in the investigation of two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged in 2003 with conspiring to provide material support to al Qaeda and HAMAS. Based upon information obtained

through an FBI undercover investigation, the complaint alleges that Al-Moayad had boasted that he had personally handed Usama Bin Laden \$20 million from his terrorist fund-raising network and that Al-Moayad and Zayed had flown from Yemen to Frankfurt, Germany, in 2003 with the intent to obtain \$2 million from a terrorist sympathizer (portrayed by a confidential informant) who wanted to fund al Qaeda and HAMAS. During their meetings, Al-Moayad and Zayed specifically promised the donor that his money would be used to support HAMAS, al Qaeda, and any other mujahideen, and "swore to Allah" that they would keep their dealings secret. Al-Moayad and Zayed were extradited to the United States from Germany in November 2003 and are currently awaiting trial.

Sections 218 and 504 were also used to gain access to intelligence that facilitated the indictment of Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation (BIF). Arnaout conspired to fraudulently obtain charitable donations in order to provide financial assistance to Chechen rebels and organizations engaged in violence and terrorism. Arnaout had a long-standing relationship with Usama Bin Laden, and used his charities both to obtain funds for terrorist organizations from unsuspecting Americans and to serve as a channel for people to contribute money knowingly to such groups. Arnaout pled guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

The broader information sharing and coordination made possible by sections 218 and 504 of the USA PATRIOT Act assisted the San Diego prosecution of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in several guilty pleas. Two defendants admitted that they had conspired to distribute approximately five metric tons of hashish and 600 kilograms of heroin originating in Pakistan to undercover United States law enforcement officers. Additionally, they admitted that they had conspired to receive, as partial payment for the drugs, four "Stinger" anti-aircraft missiles that they then intended to sell to the Taliban, an organization they knew at the time to be affiliated with al Qaeda. The lead defendant in the case is currently awaiting trial.

Sections 218 and 504 were also critical in the successful prosecution of Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq and of two counts of perjury. Before the Gulf War, Dumeisi passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United Nations. During this investigation, intelligence officers conducting surveillance of Dumeisi pursuant to FISA shared information with law enforcement agents and prosecutors investigating Dumeisi. Through this



FEDERAL BUREAU OF INVESTIGATION  
FOIPA  
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 7

Page 114 ~ Duplicate

Page 115 ~ Duplicate

Page 116 ~ Duplicate

Page 117 ~ Duplicate

Page 118 ~ Duplicate

Page 119 ~ Duplicate

Page 120 ~ Duplicate

**THOMAS, JULIE F. (OGC) (FBI)**

**From:** Caproni, Valerie E. (OGC) (FBI)  
**Sent:** Monday, November 29, 2004 12:04 PM  
**To:** THOMAS, JULIE F. (OGC) (FBI)  
**Subject:** RE: Combined Business Record/Pen Register

SENSITIVE BUT UNCLASSIFIED  
NON-RECORD

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 12-08-2005 BY 65179/DMH/LP/RW 05-CV-0845

b5

[REDACTED]

-----Original Message-----

**From:** THOMAS, JULIE F. (OGC) (FBI)  
**Sent:** Monday, November 29, 2004 11:59 AM  
**To:** Caproni, Valerie E. (OGC) (FBI)  
**Subject:** Combined Business Record/Pen Register

SENSITIVE BUT UNCLASSIFIED  
NON-RECORD

Dear Valerie,

[REDACTED]

b5  
b6  
b7C

*Julie F. Thomas  
DGC, National Security Law Branch  
Office of the General Counsel  
Room 7075*

[REDACTED]

*Julie.Thomas@ic.fbi.gov*

b2

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

11/29/2004

~~SECRET~~

THOMAS, JULIE F. (OGC) (FBI)

From: [REDACTED] (OGC) (OGA)

b6

Sent: Monday, November 29, 2004 11:38 AM

DATE: 12-12-2005

b7C

CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845

To: THOMAS, JULIE F. (OGC) (FBI)

REASON: 1.4 (c)

DECLASSIFY ON: 12-12-2030

Subject: RE: Pen Register

~~SECRET~~ (U)

RECORD 268-hq-1092598-K

thanks Julie.

b5

b6

b7C

-----Original Message-----

From: THOMAS, JULIE F. (OGC) (FBI)

Sent: Monday, November 29, 2004 10:18 AM

To: [REDACTED] (OGC) (OGA)

b6

Subject: FW: Pen Register

b7C

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

~~SECRET~~ (U)

RECORD 268-hq-1092598-K

b6

b7C

b5

-----Original Message-----

From: [REDACTED] (ITD) (FBI)

Sent: Monday, November 29, 2004 9:56 AM

To: [REDACTED] (ITD) (FBI); [REDACTED] (ITD) (FBI)

b6

Cc: THOMAS, JULIE F. (OGC) (FBI)

b7C

Subject: RE: Pen Register

~~SECRET~~ (U)

RECORD 268-hq-1092598-K

b5

Deputy General Counsel Thomas,

b6

b7C

Sorry for the delay.

SSA [REDACTED]

b6

b7C

-----Original Message-----

From: [REDACTED] (ITD) (FBI)

b6

Sent: Monday, November 08, 2004 2:25 PM

b7C

To: [REDACTED] (ITD) (FBI)

Cc: THOMAS, JULIE F. (OGC) (FBI)

Subject: FW: Pen Register Fax

~~SECRET~~ (U)

RECORD 268-hq-1092598-K

11/29/2004

~~SECRET~~

~~SECRET~~

Message

Page 2 of 2

(S)

[redacted] Deputy General Counsel Julie Thomas [redacted]  
[redacted]

b1  
b6  
b7C  
b5

[redacted]

b6  
b7C  
b2

-----Original Message-----

From: [redacted] (ITD) (FBI)  
Sent: Monday, November 08, 2004 2:02 PM  
To: [redacted] (ITD) (FBI); [redacted] (ITD) (FBI)  
Subject: Pen Register Fax

b6  
b7C

~~SECRET~~ (U)  
RECORD 268-hq-1092598-K

see attached.

~~DERIVED FROM: Single Source Document:  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~DERIVED FROM: Single Source Document  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~DERIVED FROM: Single Source Document  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~DERIVED FROM: Single Source Document  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~DERIVED FROM: Single Source Document  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

11/29/2004

~~SECRET~~

~~SECRET~~

THOMAS, JULIE F. (OGC) (FBI)

**From:** THOMAS, JULIE F. (OGC) (FBI)  
**Sent:** Monday, November 29, 2004 12:06 PM  
**To:** [REDACTED] (OGC) (OGA)  
**Subject:** RE: Pen Register

b6  
b7C

~~SECRET~~ (U)

RECORD 268-hq-1092598-K

[REDACTED] Valerie.  
 [REDACTED] Thanks, Julie

b6  
b7C

-----Original Message-----

**From:** [REDACTED] (OGC) (OGA)  
**Sent:** Monday, November 29, 2004 11:38 AM  
**To:** THOMAS, JULIE F. (OGC) (FBI)  
**Subject:** RE: Pen Register

DATE: 12-12-2005  
 CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845  
 REASON: 1.4 (c)  
 DECLASSIFY ON: 12-12-2030

b5

~~SECRET~~ (U)

RECORD 268-hq-1092598-K

thanks Julie.  
 [REDACTED]  
 [REDACTED] Soike [REDACTED] Valerie [REDACTED]  
 [REDACTED]

b6  
b7C  
b5

-----Original Message-----

**From:** THOMAS, JULIE F. (OGC) (FBI)  
**Sent:** Monday, November 29, 2004 10:18 AM  
**To:** [REDACTED] (OGC) (OGA)  
**Subject:** FW: Pen Register

ALL INFORMATION CONTAINED  
 HEREIN IS UNCLASSIFIED EXCEPT  
 WHERE SHOWN OTHERWISE

b6  
b7C

~~SECRET~~ (U)

RECORD 268-hq-1092598-K

[REDACTED] Thanks, Julie

-----Original Message-----

**From:** [REDACTED] (ITD) (FBI)  
**Sent:** Monday, November 29, 2004 9:56 AM  
**To:** [REDACTED] (ITD) (FBI) [REDACTED] (ITD) (FBI)  
**Cc:** THOMAS, JULIE F. (OGC) (FBI)  
**Subject:** RE: Pen Register

b6  
b7C  
b5

~~SECRET~~ (U)

RECORD 268-hq-1092598-K

Deputy General Counsel Thomas,

[REDACTED]

b6  
b7C  
b5

11/29/2004

~~SECRET~~

~~SECRET~~

SSA [redacted]  
[redacted]

b6  
b7C  
b2

-----Original Message-----

**From:** [redacted] (ITD) (FBI)  
**Sent:** Monday, November 08, 2004 2:25 PM  
**To:** [redacted] (ITD) (FBI)  
**Cc:** THOMAS, JULIE F. (OGC) (FBI)  
**Subject:** FW: Pen Register Fax

~~SECRET~~ (U)

RECORD 268-hq-1092598-K

(S)

b1  
b6  
b7C

[redacted] Deputy General Counsel Julie Thomas [redacted]  
[redacted]  
[redacted]

b6  
b7C  
b2

-----Original Message-----

**From:** [redacted] (ITD) (FBI)  
**Sent:** Monday, November 08, 2004 2:02 PM  
**To:** [redacted] (ITD) (FBI); [redacted] (ITD) (FBI)  
**Subject:** Pen Register Fax

b6  
b7C

~~SECRET~~

RECORD 268-hq-1092598-K

see attached.

~~DERIVED FROM: Single Source Document  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~DERIVED FROM: Single Source Document  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~DERIVED FROM: Single Source Document  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~DERIVED FROM: Single Source Document~~

11/29/2004

~~SECRET~~

~~SECRET~~

~~DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~DERIVED FROM: Single Source Document  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~DERIVED FROM: Single Source Document  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~SECRET~~

~~SECRET~~

THOMAS, JULIE F. (OGC) (FBI)

From: [REDACTED] (ITD) (FBI)  
 Sent: Monday, November 08, 2004 2:25 PM  
 To: [REDACTED] (ITD) (FBI)  
 Cc: THOMAS, JULIE F. (OGC) (FBI)  
 Subject: FW: Pen Register Fax

DATE: 12-12-2005  
 CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845  
 REASON: 1.4 (c)  
 DECLASSIFY ON: 12-12-2030

b6  
 b7C

~~SECRET~~ (U)  
 RECORD 268-hq-1092598-K

[REDACTED] Deputy General Counsel Julie Thomas [REDACTED] (S)

(S)

ALL INFORMATION CONTAINED  
 HEREIN IS UNCLASSIFIED EXCEPT  
 WHERE SHOWN OTHERWISE

b6  
 b7C  
 b1  
 b2  
 b7E  
 b5

-----Original Message-----

From: [REDACTED] (ITD) (FBI)  
 Sent: Monday, November 08, 2004 2:02 PM  
 To: [REDACTED] (ITD) (FBI) [REDACTED] (ITD) (FBI)  
 Subject: Pen Register Fax

b6  
 b7C

~~SECRET~~ (U)  
 RECORD 268-hq-1092598-K

see attached.

~~DERIVED FROM: Single Source Document  
 DECLASSIFICATION EXEMPTION 1  
 SECRET~~

~~DERIVED FROM: Single Source Document  
 DECLASSIFICATION EXEMPTION 1  
 SECRET~~

*Need by Friday*

~~SECRET~~



**THOMAS, JULIE F. (OGC) (FBI)**

**From:** THOMAS, JULIE F. (OGC) (FBI)  
**Sent:** Monday, November 08, 2004 3:33 PM  
**To:** [REDACTED] (OGC) (OGA)  
**Subject:** Delegations

b6

b7c

**UNCLASSIFIED**  
**NON-RECORD**

[REDACTED]

b6

b7c

On October 10, 2003, the authority to approve an application for business records was delegated by the Director to the Deputy Director, the EAD for Counterterrorism/Counterintelligence, the AD and all DADs of the Counterterrorism, Counterintelligence, and Cyber Divisions, the General Counsel, the Deputy General Counsel for National Security Affairs (me) and the Senior Counsel for National Security Affairs (Spike). [REDACTED]

[REDACTED]

b5

b2

Julie Thomas

[REDACTED]

**UNCLASSIFIED**

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 12-08-2005 BY 65179/DMH/LP/RW 05-CV-0845

11/8/2004



b2  
b5  
b6  
b7C

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 12-08-2005 BY 65179/DMH/LP/RW 05-CV-0845

~~SECRET~~

THOMAS, JULIE F. (OGC) (FBI)

b6

b7C

From: [REDACTED] (OGC) (FBI)  
 Sent: Thursday, October 21, 2004 11:02 AM  
 To: THOMAS, JULIE F. (OGC) (FBI)  
 Subject: FW:

SENSITIVE BUT UNCLASSIFIED  
NON-RECORD

b5

b6

b7C

Julie:

[REDACTED]

-----Original Message-----

From: [REDACTED] (OGC) (FBI)  
 Sent: Friday, October 15, 2004 12:53 PM  
 To: [REDACTED] (OGC) (FBI)  
 Subject:

ALL INFORMATION CONTAINED  
 HEREIN IS UNCLASSIFIED EXCEPT  
 WHERE SHOWN OTHERWISE

b6

b7C

SECRET

This is the information I propose to give to Julie about business records:

[REDACTED]

b5

10/21/2004

~~SECRET~~

~~SECRET~~

[Redacted]

[Redacted]

(S)

b1

[Redacted]

(S)

b1

b2

b7E

[Redacted]

b5

10/21/2004

~~SECRET~~

~~SECRET~~



b5

SENSITIVE BUT UNCLASSIFIED

10/21/2004

~~SECRET~~

~~SECRET~~

THOMAS, JULIE F. (OGC) (FBI)

b6

b7C

From: [REDACTED] (OGC) (FBI)

Sent: Thursday, October 21, 2004 11:20 AM

To: THOMAS, JULIE F. (OGC) (FBI)

Cc: [REDACTED] (OGC) (FBI)

Subject: [REDACTED] request

DATE: 12-12-2005  
CLASSIFIED BY 65179/DMH/LE/RW 05-cv-0845  
REASON: 1.4 (c)  
DECLASSIFY ON: 12-12-2030

(S)

SENSITIVE BUT UNCLASSIFIED  
NON-RECORD

b1

Julie [REDACTED]

[REDACTED]

b5

b1

(S)

[REDACTED]

-----Original Message-----

From: [REDACTED] (OGC) (FBI)

b6

Sent: Thursday, October 21, 2004 11:03 AM

b7C

To: [REDACTED] (OGC) (FBI)

Subject: RE:

SENSITIVE BUT UNCLASSIFIED  
NON-RECORD

I have forwarded to Julie. Thanks.

-----Original Message-----

From: [REDACTED] (OGC) (FBI)

Sent: Friday, October 15, 2004 12:53 PM

To: [REDACTED] (OGC) (FBI)

Subject:

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

b6

b7C

SECRET

This is the information I propose to give to Julie about business records:

[REDACTED]

b5

~~SECRET~~

10/21/2004

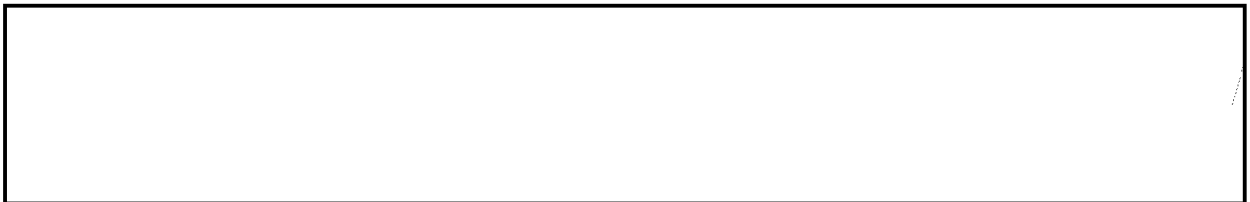
~~SECRET~~



b5



b5



(S)

b1



(S)

b1

b2

b7E

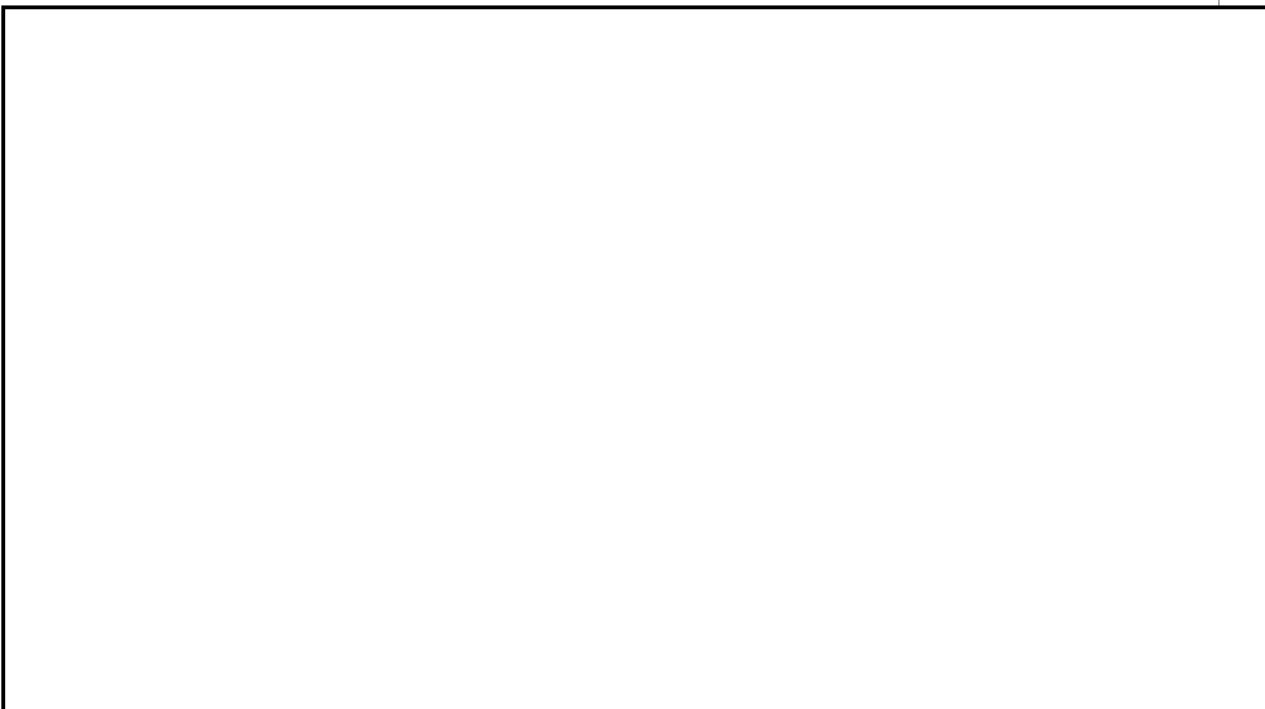


b5

10/21/2004

~~SECRET~~

~~SECRET~~



b5

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~



**THOMAS, JULIE F. (OGC) (FBI)**

**From:** [REDACTED] (OGC) (FBI)

**Sent:** Thursday, October 14, 2004 2:23 PM

**To:** THOMAS, JULIE F. (OGC) (FBI)

**Cc:** [REDACTED] (OGC) (FBI)

**Subject:** FW: Iraqi Insurgency Pleading

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 12-12-2005 BY 65179/DMH/LP/RW 05-cv-0845

SECRET

Julie --

[REDACTED]

FYI -

☐ Spike

☐ Spike

b5

[REDACTED]

[REDACTED]

b5

b6

b7C

10/14/2004

-----Original Message-----

**From:** [REDACTED] (OGC) (FBI)

**Sent:** Thursday, October 14, 2004 1:10 PM

**To:** [REDACTED] (OGC) (FBI)

b6

**Cc:** [REDACTED] (CTD) (FBI); [REDACTED] (CTD) (FBI); [REDACTED] (OGC) (FBI)

b7c

**Subject:** Iraqi Insurgency Pleading

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

SECRET

Spike, [REDACTED]

[REDACTED]

[REDACTED]

b5

[REDACTED]

**SENSITIVE BUT UNCLASSIFIED**

**SENSITIVE BUT UNCLASSIFIED**

10/14/2004

~~SECRET~~

**THOMAS, JULIE F. (OGC) (FBI)**

**From:** [REDACTED] (OGC) (FBI)

**Sent:** Friday, October 22, 2004 1:06 PM

**To:** THOMAS, JULIE F. (OGC) (FBI)

**Cc:** [REDACTED] (OGC) (FBI)

**Subject:** business records

DATE: 12-12-2005  
CLASSIFIED BY 65179/DMH/LP/RW 05-cv-0845  
REASON: 1.4 (c)  
DECLASSIFY ON: 12-12-2030

b6  
b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

Here is a copy of the powerpoint on national security letters, business records, etc.

(S)

b1  
b2  
b7E  
b6  
b7C

**SENSITIVE BUT UNCLASSIFIED**

~~SECRET~~

10/25/2004

# FISA - Business Records

- Patriot Act expanded universe of items obtainable, to “any tangible things (including books, records, papers, documents and other items)”
- Patriot Act changed legal standard: “the information to be obtained is foreign intelligence information not concerning a US person, or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence gathering activities” and investigation of USP cannot be based solely on activities protected by First Amendment
- Same standard as established by Patriot Act for PR/TT; NSLs
- Available in PI and full investigations

~~SECRET~~

~~SECRET~~

# FISA - Business Records

- FISA permits delegation down to level of ASAC
- At current time, approval authority has been delegated to headquarters officials (Deputy Director; EAD for CT/CI; AD and all DADs of CT, CI, Cyber; General Counsel, Deputy General Counsel for National Security Affairs, and Senior Counsel for National Security Affairs)
- Business records form available for field to fill out and submit to headquarters and NSLB (atty )

b6  
b7c

~~SECRET~~

# FISA - Business Records

(S)

- We will be sending out guidance on service of the order, since it is classified and most recipients will not be cleared.

b1

~~SECRET~~

~~SECRET~~

[REDACTED] (OGC) (FBI)

b6

b7C

From: [REDACTED] (OGC) (FBI)

Sent: Wednesday, November 10, 2004 1:46 PM

b6

To: THOMAS, JULIE F. (OGC) (FBI); [REDACTED] (OGC) (FBI)

b7C

Subject: [REDACTED] quest  
(S)

DATE: 12-12-2005  
CLASSIFIED BY 65179/DMH/LP/RW 05-cv-0645  
REASON: 1.4 (C)  
DECLASSIFY ON: 12-12-2030

SENSITIVE BUT UNCLASSIFIED  
NON-RECORD

(S)

[REDACTED]

b1

b2

b7E

(S)

[REDACTED]

All in all, I guess we should go along with this. But this is no longer an FBI document, it's an OIPR document, and I don't like that fact.

[REDACTED]

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

Although I haven't broached the subject with OIPR since Julie's discussion with Baker, it appears from the fact that we have copies that OIPR says are ready to go indicates [REDACTED]

b5

b6

b7C

SENSITIVE BUT UNCLASSIFIED

11/10/2004

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION  
FOIPA  
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 136

Page 2 ~ Referral/Direct  
Page 3 ~ Referral/Direct  
Page 4 ~ Referral/Direct  
Page 5 ~ Referral/Direct  
Page 6 ~ Referral/Direct  
Page 7 ~ Referral/Direct  
Page 8 ~ Referral/Direct  
Page 9 ~ Referral/Direct  
Page 10 ~ Referral/Direct  
Page 11 ~ Referral/Direct  
Page 21 ~ Referral/Direct  
Page 22 ~ Referral/Direct  
Page 23 ~ Referral/Direct  
Page 24 ~ Referral/Direct  
Page 25 ~ Referral/Direct  
Page 26 ~ Referral/Direct  
Page 27 ~ Referral/Direct  
Page 28 ~ Referral/Direct  
Page 29 ~ Referral/Direct  
Page 30 ~ Referral/Direct  
Page 31 ~ Referral/Direct  
Page 32 ~ Referral/Direct  
Page 33 ~ Referral/Direct  
Page 34 ~ Referral/Direct  
Page 35 ~ Referral/Direct  
Page 36 ~ Referral/Direct  
Page 37 ~ Referral/Direct  
Page 38 ~ Referral/Direct  
Page 39 ~ Referral/Direct  
Page 40 ~ Referral/Direct  
Page 41 ~ Referral/Direct  
Page 42 ~ Referral/Direct  
Page 43 ~ Referral/Direct  
Page 44 ~ Referral/Direct  
Page 45 ~ Referral/Direct  
Page 46 ~ Referral/Direct  
Page 47 ~ Referral/Direct  
Page 48 ~ Referral/Direct  
Page 49 ~ Referral/Direct  
Page 50 ~ Referral/Direct  
Page 51 ~ Referral/Direct  
Page 52 ~ Referral/Direct  
Page 53 ~ Referral/Direct  
Page 54 ~ Referral/Direct



Page 55 ~ Referral/Direct  
Page 56 ~ Referral/Direct  
Page 57 ~ Referral/Direct  
Page 58 ~ Referral/Direct  
Page 59 ~ Referral/Direct  
Page 60 ~ Referral/Direct  
Page 61 ~ Referral/Direct  
Page 65 ~ Referral/Direct  
Page 66 ~ Referral/Direct  
Page 67 ~ Referral/Direct  
Page 68 ~ Referral/Direct  
Page 69 ~ Referral/Direct  
Page 70 ~ Referral/Direct  
Page 71 ~ Referral/Direct  
Page 72 ~ Referral/Direct  
Page 73 ~ Duplicate  
Page 74 ~ Duplicate  
Page 75 ~ Duplicate  
Page 76 ~ Duplicate  
Page 77 ~ Duplicate  
Page 78 ~ Duplicate  
Page 79 ~ Duplicate  
Page 106 ~ Referral/Direct  
Page 124 ~ Referral/Direct  
Page 125 ~ Referral/Direct  
Page 126 ~ Referral/Direct  
Page 127 ~ Referral/Direct  
Page 128 ~ Referral/Direct  
Page 129 ~ Referral/Direct  
Page 130 ~ Referral/Direct  
Page 131 ~ Referral/Direct  
Page 132 ~ Referral/Direct  
Page 133 ~ Referral/Direct  
Page 134 ~ Referral/Direct  
Page 135 ~ Referral/Direct  
Page 136 ~ Duplicate  
Page 137 ~ Referral/Direct  
Page 138 ~ Referral/Direct  
Page 139 ~ Referral/Direct  
Page 140 ~ Referral/Direct  
Page 141 ~ Duplicate  
Page 142 ~ Duplicate  
Page 143 ~ Duplicate  
Page 144 ~ Referral/Direct  
Page 145 ~ Referral/Direct  
Page 147 ~ Duplicate  
Page 148 ~ Duplicate  
Page 149 ~ Duplicate  
Page 150 ~ Duplicate  
Page 151 ~ Duplicate  
Page 152 ~ Duplicate

Page 153 ~ Duplicate  
Page 154 ~ Duplicate  
Page 155 ~ Duplicate  
Page 156 ~ Duplicate  
Page 157 ~ Duplicate  
Page 158 ~ Duplicate  
Page 159 ~ Duplicate  
Page 160 ~ Duplicate  
Page 161 ~ Duplicate  
Page 162 ~ Duplicate  
Page 163 ~ Duplicate  
Page 164 ~ Duplicate  
Page 165 ~ Duplicate  
Page 166 ~ Duplicate  
Page 167 ~ Duplicate  
Page 168 ~ Duplicate  
Page 169 ~ Duplicate  
Page 170 ~ Duplicate  
Page 171 ~ Duplicate  
Page 172 ~ Duplicate  
Page 173 ~ Duplicate  
Page 174 ~ Referral/Direct  
Page 175 ~ Referral/Direct  
Page 176 ~ Referral/Direct  
Page 177 ~ Referral/Direct  
Page 178 ~ Referral/Direct  
Page 179 ~ Referral/Direct  
Page 180 ~ Referral/Direct  
Page 181 ~ Referral/Direct  
Page 182 ~ Referral/Direct  
Page 183 ~ Referral/Direct  
Page 184 ~ Referral/Direct  
Page 185 ~ Referral/Direct  
Page 186 ~ Referral/Direct  
Page 187 ~ Referral/Direct  
Page 188 ~ Referral/Direct  
Page 189 ~ Referral/Direct  
Page 190 ~ Referral/Direct  
Page 191 ~ Referral/Direct  
Page 192 ~ Referral/Direct  
Page 193 ~ Referral/Direct

~~SECRET~~

DATE: 12-05-2005

FBI INFO.

CLASSIFIED BY 65179 DMH/LP/DPW

REASON: 1.4 ((C) 05-CV-0845)

DECLASSIFY ON: 12-05-2030

b6

b7C

**From:** [REDACTED] (CTD) (FBI)

**Sent:** Thursday, March 31, 2005 1:01 PM

**To:** HEIMBACH, MICHAEL J. (CTD) (FBI); [REDACTED] (CTD) (FBI); HULON, WILLIE T. (CTD) (FBI)

**Cc:** HQ-DIV13-ITOS I

**Subject:** Patriot Act Roving Authority - ITOS1 response

**SECRET**

**RECORD n/a**

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

Hello,

(S) [REDACTED]

[REDACTED]

b1

(S) [REDACTED]

b2

b7E

[REDACTED]

b5

Example:

(U) [REDACTED]

b2

[REDACTED]

b7D

b7E

[REDACTED]

CTD/ITOS-1

FBIHQ

desk:

page:

[REDACTED]

b2

[REDACTED]

b6

[REDACTED]

b7C

-----Original Message-----

**From:** HULON, WILLIE T. (CTD) (FBI)

**Sent:** Wednesday, March 30, 2005 9:24 PM

**To:** Caproni, Valerie E. (OGC) (FBI); VANNUYS, THOMAS J. (CTD) (FBI); HEIMBACH, MICHAEL J. (CTD) (FBI)

**Subject:** RE: Help

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

Tom/Mike,

Please provide info re this by noon, Thursday.

Thanks

Willie T.

~~SECRET~~

-----Original Message-----

**From:** Caproni, Valerie E. (OGC) (FBI)

b6

b7C

~~SECRET~~

**Sent:** Wednesday, March 30, 2005 6:51 PM

**To:** BALD, GARY M. (DO) (FBI); HULON, WILLIE T. (CTD) (FBI); SZADY, DAVID (CD) (FBI);  
PISTOLE, JOHN S. (DO) (FBI); FEDARCYK, MICHAEL R. (DO) (FBI)

**Cc:** KALISCH, ELENI P. (OCA) (FBI)

**Subject:** Help

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

(S)

In the draft of testimony for the AG, they are



b1

b2

b7E

b5

**SENSITIVE BUT UNCLASSIFIED**

~~**DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations**~~  
~~**DECLASSIFICATION EXEMPTION 1**~~

~~**SECRET**~~

~~SECRET~~

b6

b7C

~~SECRET~~

**From:** [REDACTED] (CTD) (FBI)  
**Sent:** Thursday, March 17, 2005 4:51 PM  
**To:** HEIMBACH, MICHAEL J. (CTD) (FBI)  
**Cc:** [REDACTED] (OGC) (FBI)  
**Subject:** RE: Patriot Act & library records

b6

b7C

b6

b7C

DATE: 12-05-2005  
 CLASSIFIED BY 65179 DMH/LP/DFW  
 REASON: 1.4 ((C), 05-CV-0845)  
 DECLASSIFY ON: 12-05-2030

~~SECRET~~  
 RECORD [REDACTED]

The answer is: b2

ALL INFORMATION CONTAINED  
 HEREIN IS UNCLASSIFIED EXCEPT  
 WHERE SHOWN OTHERWISE

- Requests pursuant to the Patriot Act business records/library records provision would be executed via NSIs

[REDACTED]

(S)

Ta-da. Thanks [REDACTED]

b6

b7C

b1

b2

b7E

b5

[REDACTED]  
 CTD/ITOS-1

FBIHQ [REDACTED]

desk [REDACTED]

pager [REDACTED]

b2

b6

b7C

-----Original Message-----

**From:** HEIMBACH, MICHAEL J. (CTD) (FBI)

**Sent:** Thursday, March 17, 2005 11:56 AM

**To:** [REDACTED] (CTD) (FBI)

b6

**Subject:** FW: Patriot Act

b7C

UNCLASSIFIED

NON-RECORD

See if this is something we track and/or can retrieve. Thanks Mike

Section Chief Michael J. Heimbach

CTD/ITOS I

Office # 571-280-5267

Pager # [REDACTED]

Cell # [REDACTED]

b2

b6

b7C

-----Original Message-----

**From:** [REDACTED] (CTD) (FBI)

**Sent:** Thursday, March 17, 2005 11:48 AM

**To:** [REDACTED] (CTD) (FBI); HEIMBACH, MICHAEL J. (CTD) (FBI); VANNUYS, THOMAS J. (CTD) (FBI)

**Cc:** VAN DUYN, DONALD N. (CTD) (FBI)

**Subject:** FW: Patriot Act

~~SECRET~~

b6

b7C

~~SECRET~~

**UNCLASSIFIED**  
**NON-RECORD**

[REDACTED]

b6

b7C

Please look at the request below from EAD Bald, which came to us through AD Hulon. Is this somehow picked up on the scorecard you generate for the visiting SACs?

Mike & Tom,

Is this something that either of the ITOS units monitor?

Thank You,

b6

[REDACTED]

b7C

-----Original Message-----

**From:** HULON, WILLIE T. (CTD) (FBI)

b6

**Sent:** Thursday, March 17, 2005 11:27 AM

b7C

**To:** [REDACTED] (CTD) (FBI)

**Cc:** BALD, GARY M. (DO) (FBI); [REDACTED] (CTD) (FBI); [REDACTED] (CTD) (FBI); [REDACTED] (DO) (FBI)

**Subject:** FW: Patriot Act

**UNCLASSIFIED**  
**NON-RECORD**

b6

[REDACTED]

b7C

Please determine if there is a mechanism for determining the instances when the use of the Patriot Act 215 has been employed in CT matters. If so, please provide the stats.

Thanks

Willie T.

-----Original Message-----

**From:** BALD, GARY M. (DO) (FBI)

**Sent:** Thursday, March 17, 2005 8:32 AM

**To:** REIGEL, LOUIS M. (CyD) (FBI); HULON, WILLIE T. (CTD) (FBI); Caproni, Valerie E. (OGC) (FBI)

**Cc:** PISTOLE, JOHN S. (DO) (FBI); STEELE, CHARLES M (DO)(FBI)

**Subject:** Patriot Act

**UNCLASSIFIED**  
**NON-RECORD**

Lou - This morning, the Director asked Dave Thomas, CyD for details concerning the number of times library computers have been used to launch cyber attacks. In particular, he wants this information in anticipation of questions that will arise during consideration of the sunset clauses in the Patriot Act. Would you please follow-up with Dave on this request, and include me in the response, which should be sent to the Director through Charlie Steele.

In addition, I believe it would be helpful to reliably determine [REDACTED]

[REDACTED] If the information is available in either CTD or OGC, would you, Willie and Val, please also forward this to Charlie (cc to me).

Val - If we do not currently require [REDACTED]

[REDACTED]

Thx. Gary

b6

b7C

~~SECRET~~

b2

b7E

b5

~~SECRET~~

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

~~DERIVED FROM: G-3 FBI Classification Guide G-3, dated 1/97, Foreign CounterIntelligence Investigations  
DECLASSIFICATION EXEMPTION 1  
SECRET~~

~~SECRET~~

b6

b7C

Message

~~SECRET~~

Page 1 of 3

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 12-05-2005 BY 65179 DMH/LP/DFW 05-CV-0845

**From:** [REDACTED] (CTD) (FBI)  
**Sent:** Thursday, March 17, 2005 12:43 PM b6  
**To:** HEIMBACH, MICHAEL J. (CTD) (FBI) b7C  
**Cc:** [REDACTED] (OGC) (FBI)  
**Subject:** RE: Patriot Act

DATE: 12-08-2005  
CLASSIFIED BY 65179DMH/LP/cpb 05-cv-0845  
REASON: 1.4 (c)  
DECLASSIFY ON: 12-08-2030

**UNCLASSIFIED**  
**NON-RECORD**

(S)

[REDACTED] There is no tracking method for that  
specifically in ITOS1, [REDACTED]

b1

b5

I spoke to NSLB and they are going to double-check to confirm that [REDACTED]  
[REDACTED] I spoke to [REDACTED] who noted [REDACTED]  
[REDACTED] I'll get back to  
you as soon as I get confirmation of the above.

b2

b7E

b6

b7C

[REDACTED]  
CTD/ITOS-1  
FBIHQ [REDACTED] b2  
desk: [REDACTED] b6  
pager: [REDACTED] b7C

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

-----Original Message-----

**From:** HEIMBACH, MICHAEL J. (CTD) (FBI)  
**Sent:** Thursday, March 17, 2005 11:56 AM b6  
**To:** [REDACTED] (CTD) (FBI) b7C  
**Subject:** FW: Patriot Act

**UNCLASSIFIED**  
**NON-RECORD**

See if this is something we track and/or can retrieve. Thanks Mike

Section Chief Michael J. Heimbach

CTD/ITOS I

Office # 571-280-5267

Pager # [REDACTED]

Cell # [REDACTED]

b2

b6

-----Original Message-----

**From:** [REDACTED] (CTD) (FBI) b7C  
**Sent:** Thursday, March 17, 2005 11:48 AM  
**To:** [REDACTED] (CTD) (FBI); HEIMBACH, MICHAEL J. (CTD) (FBI); VANNUYS, THOMAS J. (CTD) (FBI)  
**Cc:** VAN DUYN, DONALD N. (CTD) (FBI)  
**Subject:** FW: Patriot Act

**UNCLASSIFIED**  
**NON-RECORD**



~~SECRET~~

b6

b7C



FEDERAL BUREAU OF INVESTIGATION  
FOIPA  
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 2

Page 8 ~ Duplicate

Page 9 ~ Duplicate

[redacted] OGC) (FBI)

From: [redacted] b6  
Sent: Monday, October 20, 2003 9:39 AM b7C  
To: [redacted]  
Subject: Fwd: Re: Business Records

DECLASSIFIED BY 65179 DMH/CLS  
ON 09-03-2005

CA# 05-CV-0845

Forwarded Mail received from: [redacted]

-----Original Message-----

Date: 10/16/2003 03:48 pm -0400 (Thursday)  
From: [redacted]  
To: [redacted]

b6

b7C

CC: BOWMAN, MARION, Rowan, J  
Subject: Re: Business Records

Thanks for teeing up this issue - again. Rather than dragging their collective feet or setting up hurdles - OIPR should be embarrassed that the FBI has used this valuable tool to fight terrorism - exactly ZERO times. The inability of FBI investigators to use this seemingly effective tool has had a direct and clearly adverse impact on our terrorism cases. Quite frankly, Agents have spent the last 2 years screwing around with weak NSLs or using made up "voluntary" NSLs literally begging people to give us information in our terrorism cases (try to get info from [redacted]). The fact that this new FISA b2 tool has languish for two years - with no likely usage in the future - is nuts. While b7E radical militant librarians kick us around - true terrorists benefit from OIPR's failure to let us use the tools given to us. THIS SHOULD BE AN OIPR PRIORITY!!!

In any event - the efforts of NSLb to get this on track are greatly appreciated. (PS - don't forget OIPR's [redacted] the same story)

-----  
WFO Office of Division Counsel [redacted]

b6

Privileged and Confidential

b7C

b2

>>> [redacted] 10/16 2:56 PM >>>

Not surprisingly, we (I should say, Pat Rowan) presented OIPR with a finalized application and proposed order for business records, signed by Valerie, and they were all up in arms because we had not coordinated in advance and had not used the form they had and because we are not authorized to appear before the court and they don't have enough information about the target and . . . I guess, mainly, they were upset because we wanted to accomplish something without their interference. After Pat went through all their grievances and asked whether they would file something that used their form and met their informational needs, [redacted] said that it would depend on OIPR priorities. Which means, I guess, that we get business records after the last of the initiations sitting on their desks has been filed.

Anyway, does anyone have or has anyone heard of a business records form that OIPR has already produced. [redacted] said that [redacted] would have it but then conceded that he probably would not. Also, per FISC Rule 9, we are told that we cannot file something with the court or cannot appear in Court unless we are on some authorized list. Does anyone have a copy of the FISC rules?

I guess it was too good to be true, that we would actually be able to file something with the FISA Court with our names on it and without it being held up by OIPR.

More on this saga to come . . .

[redacted] b6

b7C

Message

b6  
b7C

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 09-08-2005 BY 65179 DMH/CLS  
CA# 05-CV-0845

Page 1 of 1

[REDACTED] (OGC) (FBI)

From: [REDACTED] (Div09) (FBI)

Sent: Friday, May 21, 2004 12:04 PM

To:

[REDACTED]

b6  
b7C

Subject: MIRACLES

UNCLASSIFIED  
NON-RECORD

UNCLASSIFIED  
NON-RECORD

We got out first business record order signed today! It only took two and a half years.

[REDACTED]

b6  
b7C

UNCLASSIFIED

UNCLASSIFIED

6/8/2005

## FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/6/2003

To: All Divisions

Attn: ADIC, AD, DAD, SAC, CDC

From: Office of the General Counsel  
National Security Law Unit

Contact: [REDACTED]

Approved By: Mueller Robert S III

b2

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 09-27-2005 BY 65179 DMH/CLS

Drafted By: [REDACTED]

b6

CA# 05-CV-0845

Case ID #: 66F-HQ-A1247863

b7C

Title: FISA BUSINESS RECORD APPLICATIONS  
DELEGATION OF AUTHORITY

Synopsis: Delegates signature authority for Applications for  
Business Records to FBIHQ officials under 50 U.S.C. § 1861.

Details: The Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C § 1861, provides for access to certain business records for foreign intelligence (FI) and international terrorism (IT) investigations through issuance of an order from the FISA Court (FISC). Section 1861(a)(1) authorizes the "Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge)" to make an application for the order.

Thus, as permitted by 50 U.S.C. § 1861(a)(1), I hereby designate certification signature authority for applications for FISA business records to the following FBI Officials:

1. The Deputy Director;
2. The Executive Assistant Director for Counterterrorism/Counterintelligence;
3. The Assistant Directors and all Deputy Assistant Directors of the Counterterrorism, Counterintelligence, and Cyber Divisions; and
4. The General Counsel; the Senior Counsel for National Security Affairs; and the Deputy General Counsel for National Security Affairs.

To: All Divisions From: Office of the General Counsel  
Re: 66F-HQ, 06/6/2003

The National Security Law Unit is hereby authorized to prepare business record applications and will issue guidance on the application process.

LEAD:

Set Lead 1: (adm)

ALL RECEIVING OFFICES

Disseminate to personnel involved in CI, IT, and Cyber operations and to other personnel as appropriate.

CA# 05-CV-0845

[REDACTED] (OGC) (FBI)

**From:**

**Sent:**

b6

Wednesday, February 25, 2004 10:17 AM

**To:**

b7C

**Subject:**

FW: Simultaneous use of criminal and FISA instruments

-----Original Message-----

**From:**

Caproni, Valerie E.

**Sent:**

Tuesday, February 24, 2004 5:29 PM

**To:**

Curran, John F; BOWMAN, MARION E.; [REDACTED]

b6

**Cc:**

[REDACTED] MUELLER, ROBERT S. III; WAINSTEIN, KENNETH L.

b7C

**Subject:**

Simultaneous use of criminal and FISA instruments

Effective immediately DOJ is no longer objecting to the simultaneous use of criminal and FISA tools. Please pass this along to all the NSLU attorneys promptly. [REDACTED]

VC

b5

~~SECRET~~

## FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/07/2003

To: Counterterrorism

Attn: SSA [REDACTED]  
SSA [REDACTED]  
IOS [REDACTED]

b2  
b6  
b7C

From: Office of the General Counsel  
National Security Law Unit (NSLU)/Room [REDACTED]  
Contact: [REDACTED]

DECLASSIFIED BY 65179 DMH/CLS  
ON 09-27-2005

Approved By: Bowman M. E.

Drafted By: [REDACTED]

Case ID #: (U) 66F-HQ-A1247863 (None)

b6  
b7C

Title: (U) [REDACTED]

Synopsis: ~~(S)~~(U) This communication conveys NSLU authorization to declassify certain FISA-derived documents for use by the U.S. Attorney's Office for [REDACTED] in criminal proceedings of [REDACTED]

~~(S)~~ Derived From: Multiple Sources (U)  
Declassify On: X1

Reference: ~~(S)~~(U) 199N-SE-85481 (Pending)

Details: ~~(S)~~(U) Pursuant to a request from the International Terrorism Operations Section I, CONUS 2, Team 7, NSLU reviewed FISA-derived material contained in a memorandum dated 02/12/2003 from FBI Assistant Director Larry Mefford to [REDACTED] Counsel, Office of Intelligence Policy and Review, Department of Justice. The memorandum was seeking authorization from the Attorney General to use information obtained or derived from the electronic surveillance and physical searches of [REDACTED] in any and all phases of criminal prosecution. NSLU reviewed the documents and determined that the cuts contained in the 02/12/2003 memorandum could be declassified. NSLU received confirmation from CONUS 2 that none of the information reviewed came from [REDACTED] surveillance of [REDACTED]

b6  
b7C

b2  
b7E

~~SECRET~~

~~SECRET~~

To: Counterterrorism From: Office of the General Counsel  
Re: (U) 66F-HQ-A1247863, 03/07/2003

LEAD(s):

Set Lead 1: (Adm)

COUNTERTERRORISM

AT WASHINGTON, D.C.

(U) Authorization provided by NSLU for the  
declassification of certain documents associated with the  
criminal prosecution of [REDACTED]

CC: 1 - Mr. Bowman

1 - [REDACTED]

b6

b7C

♦♦

~~SECRET~~



CA# 05-CV-0845

[redacted] OGC) (FBI)

From: [redacted]  
Sent: Thursday, October 09, 2003 1:46 PM  
To: [redacted]

b6  
b7C

Cc: [redacted]  
Subject: FW: [redacted] FISA Issue

b2

Forwarded FYI is WFO's response to a complaint that [redacted] was<sup>b7E</sup> processing FISA warrant searches in a timely or complete manner. Should you become aware of a similar complaint in the future I recommend that you contact [redacted] and let him check it out. He was very helpful and timely in his response.

b6

b7C

b2

b7E

-----Original Message-----

From: [redacted]  
Sent: Thursday, October 09, 2003 1:27 PM  
To: [redacted]  
Cc: [redacted]; ROWMAN, MARION E.; [redacted]

Subject: [redacted] FISA Issue

Kevin Carter, OGC

b2

At NSLB/OGC's request - WFO reviewed the nature of our relationship with [redacted] b7E  
Based on contact with the WFO squad (A-2) that serves orders to [redacted] and the supervisors of that program - WFO identified no systemic or pervasive problems with [redacted] compliance. IA [redacted] was specifically contacted and she advised that her relationship with [redacted] is excellent. With respect to the specific FISA order you identified, WFO determined that the delay was due to a initial misreading of the order by [redacted] which was rectified when brought to their attention. If FBIHQ learns of other information suggesting that problems exist - WFO will promptly address as they are reported to WFO. Again - because [redacted] is an important WFO liaison contact - it is the ADIC WFO policy that any complaints or concerns relating to [redacted] be handled in coordination with WFO. b6 b7C

The WFO POCs for issues concerning [redacted] are WFO Administrative ASAC (Brian Fortin - acting) for administrative or problem matters, CDC [redacted] for legal issues, and supervisor [redacted] (A-2) for service issues.

Finally - [redacted] is well aware of the delay in the DOJ processing of FISA orders and they will be the first to point out that they usually receive FISA orders significantly after the date signed by the FISC.

WFO Office of Division Counsel [redacted]

b2

b6

~~Privileged and Confidential~~

b7C

[redacted] OGC) (FBI)

From: [redacted] (OGC) (FBI)

Sent: Monday, August 23, 2004 5:19 PM b6

To: [redacted] (OGC) (FBI) b7C

Subject: 2702 Issue

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-03-2005 BY 65179 DMH/CLS

CA# 05-CV-0845

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

[redacted] Can you help with a matter of concern to [redacted]. He believes that the [redacted] is an invaluable resource to the Bureau. He therefore likes to try and help [redacted] whenever he can. From time to time, [redacted] pass along [redacted]

b2

[redacted] The threat is potential loss of life from an attack. [redacted] has been complaining that [redacted] provides great service but [redacted] is problematic in that [redacted]

b7E

b6

Can you please follow up on this in a few ways? Talk to [redacted] (I spoke with him once about this) and see what information he has about [redacted] compliance. You may also want to speak with [redacted] to see what knowledge they may have about compliance. Second, I'm a bit concerned that this may be a misuse of 2702 authority. If the requests from [redacted] have a clear nexus to FBI cases and they are bona fide emergencies, then I am okay with it. If, however, we are doing this purely for [redacted] and doing it for [redacted] on a routine basis, then I think it could be a problem. [redacted] of ILU has issued some guidance on 2702. See me if you do not have it. Can you do some research on 2702 (in addition to finding out what the problems are with [redacted] and prepare a memo for [redacted] on proper use of the tool, including whatever you find out about [redacted]. Please let me know if you have any questions. Thanks.

b7C

b7D

**SENSITIVE BUT UNCLASSIFIED**

6/9/2005

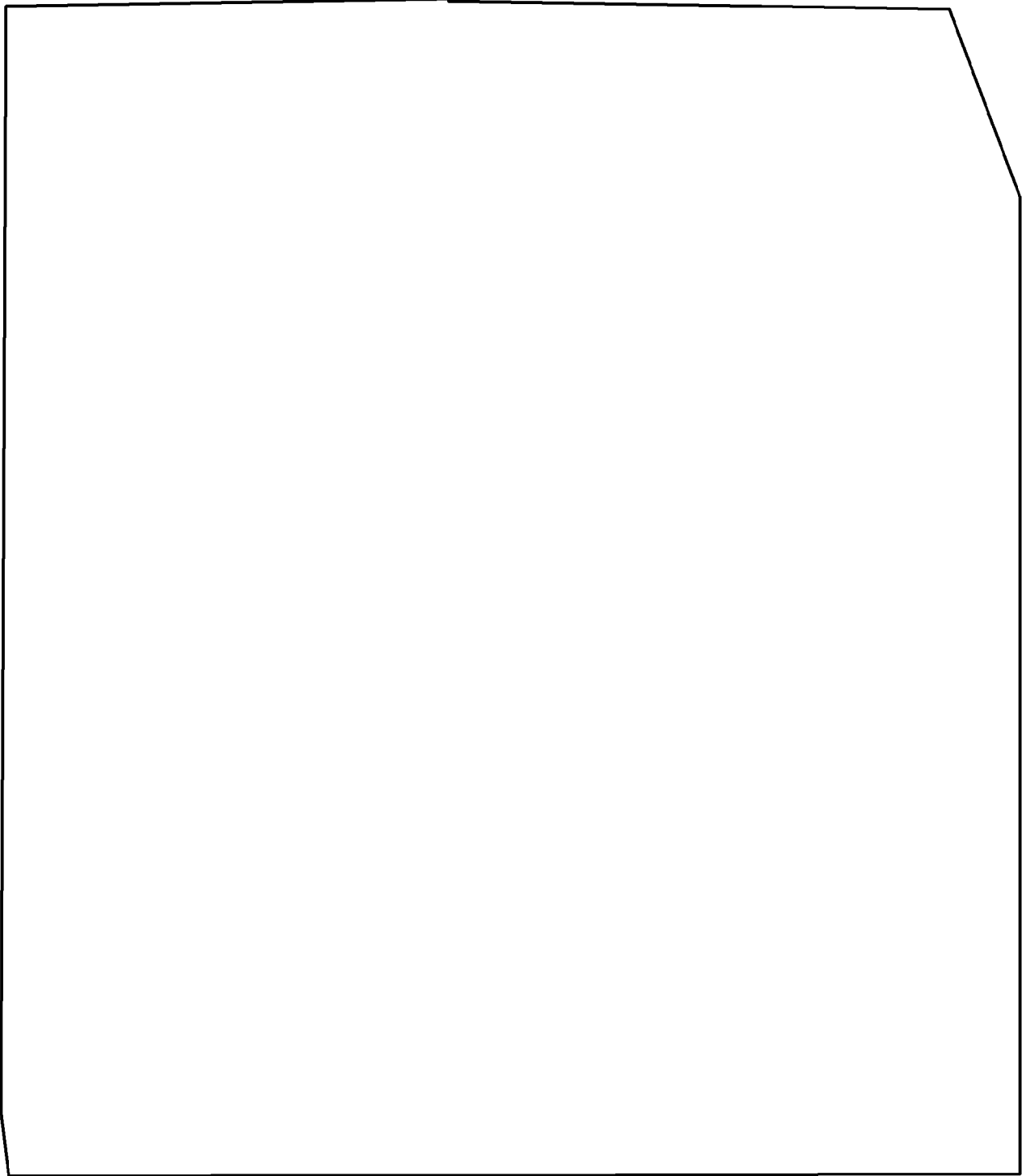
# FEDERAL BUREAU OF INVESTIGATION

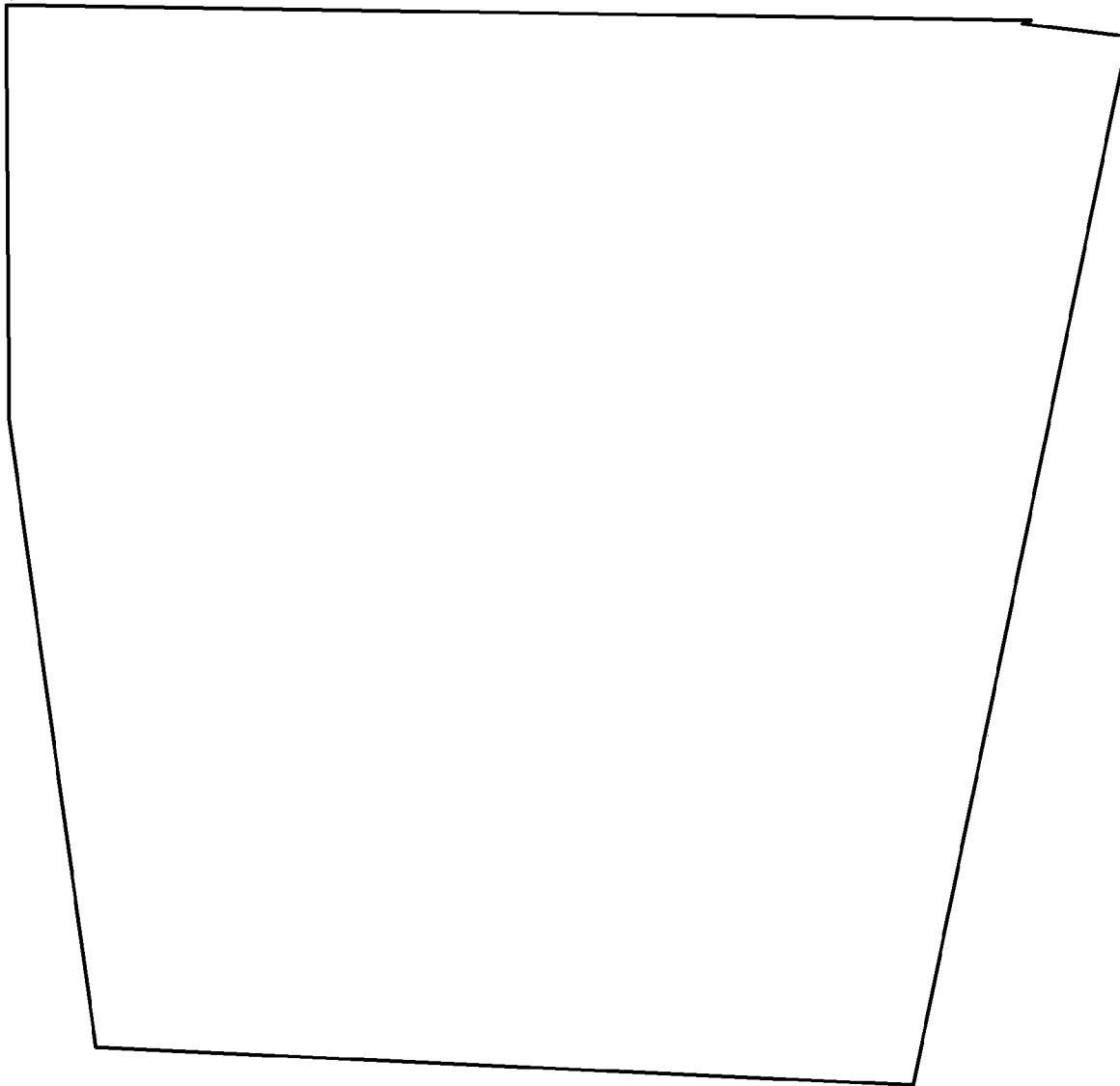
ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-03-2005 BY 65179 DMH/CLS  
CA# 05-CV-0845

b5

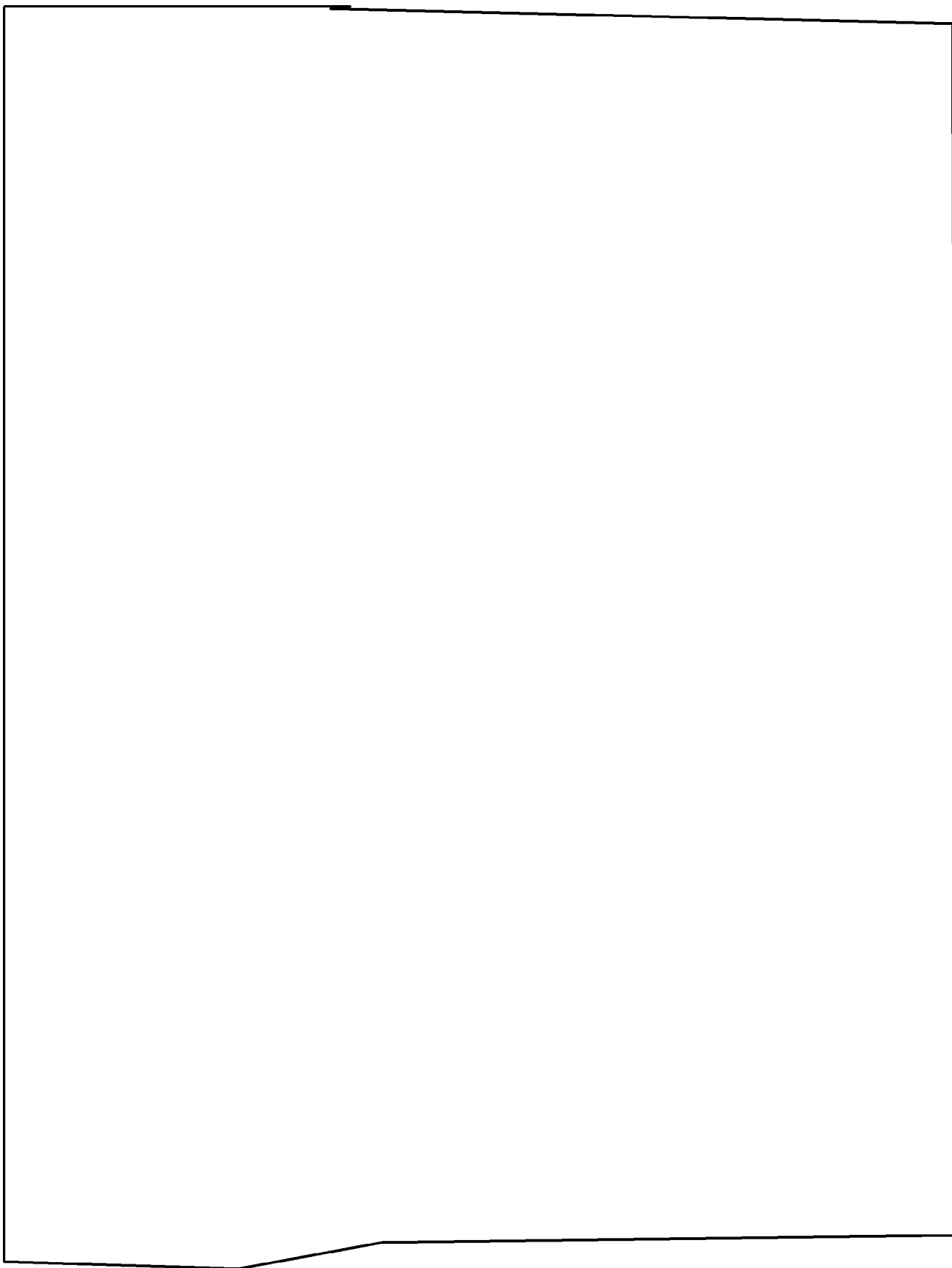
b6

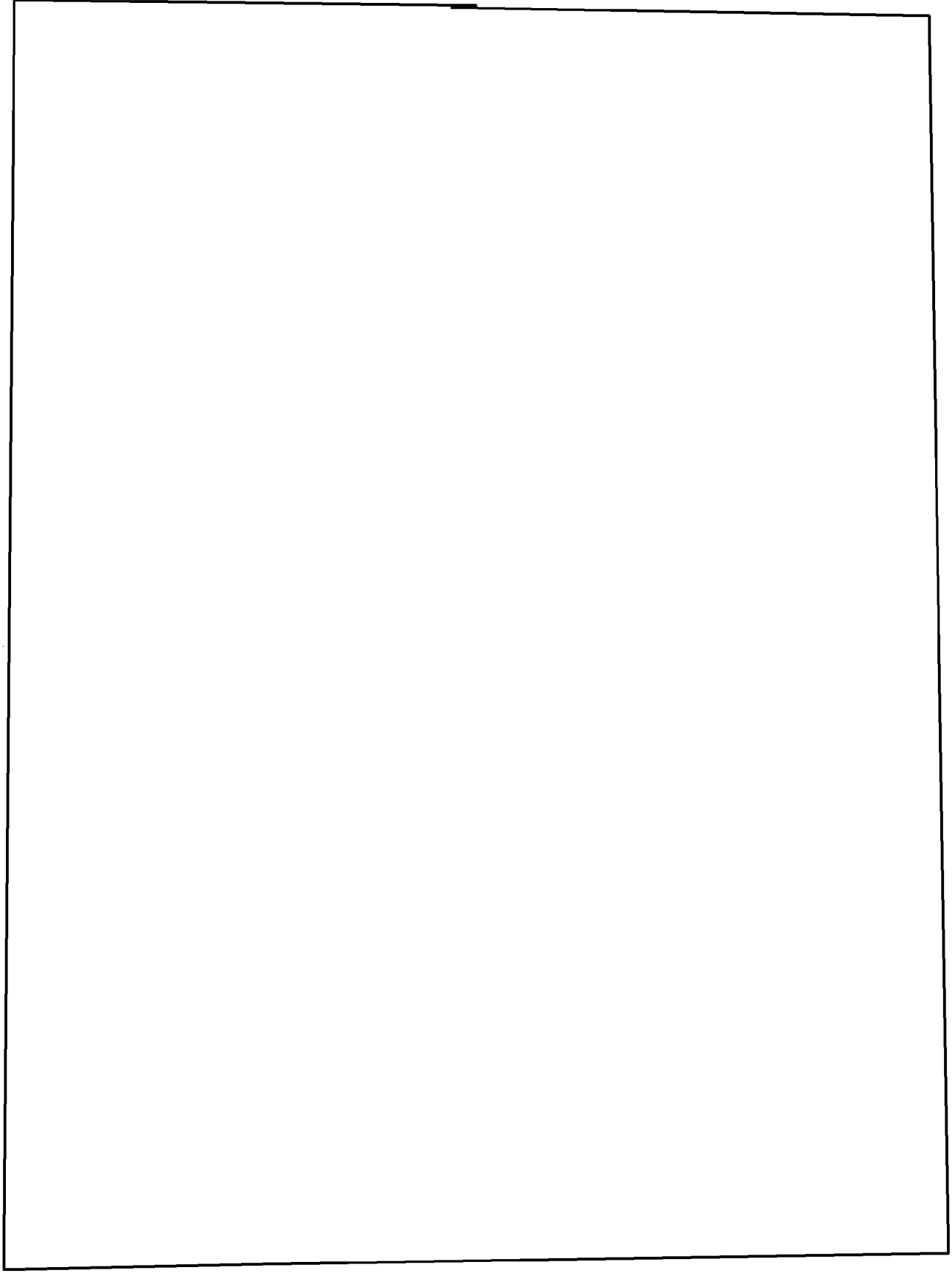
b7C

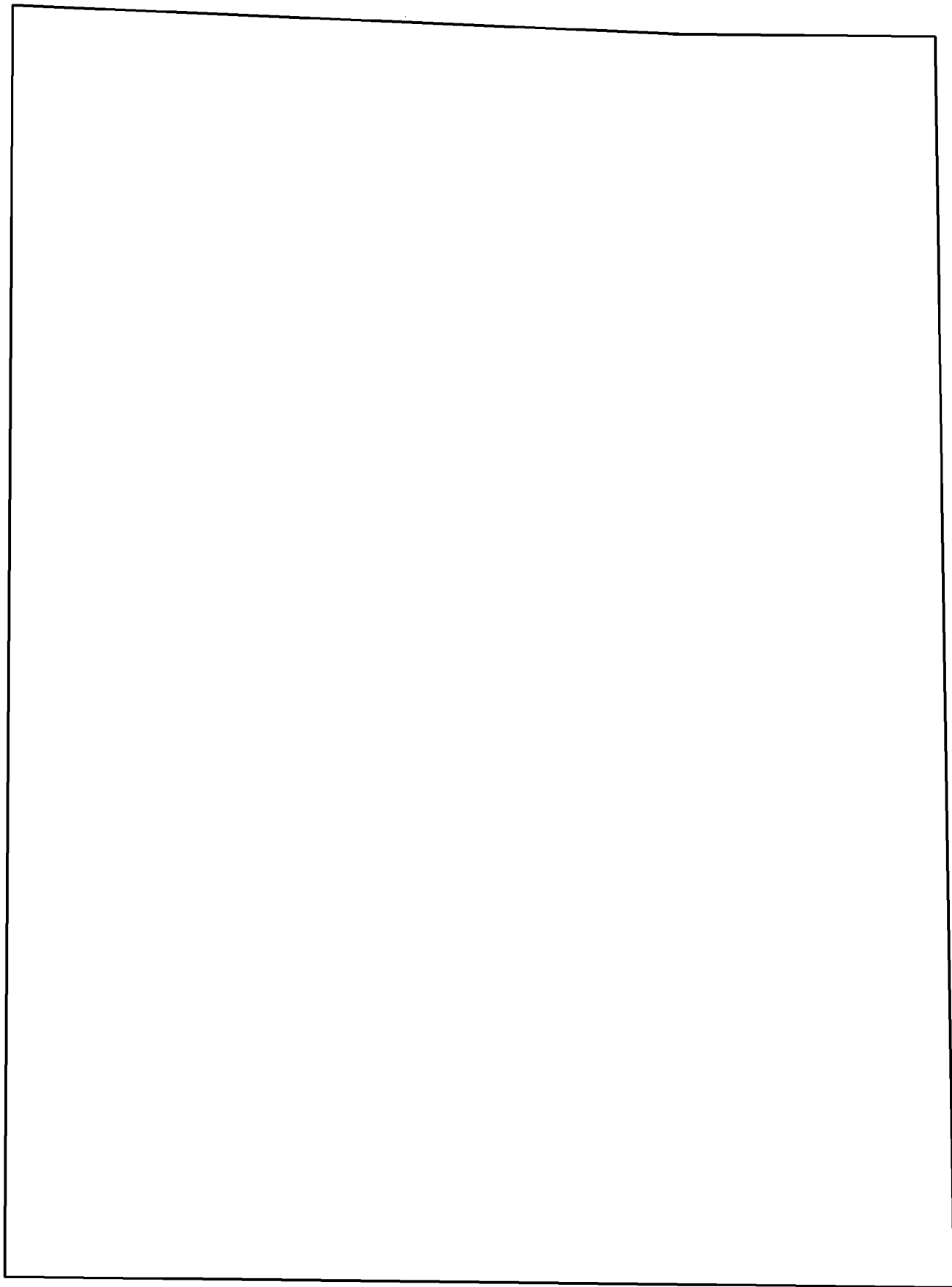




b5  
b6  
b7C











**U.S. Department of Justice**

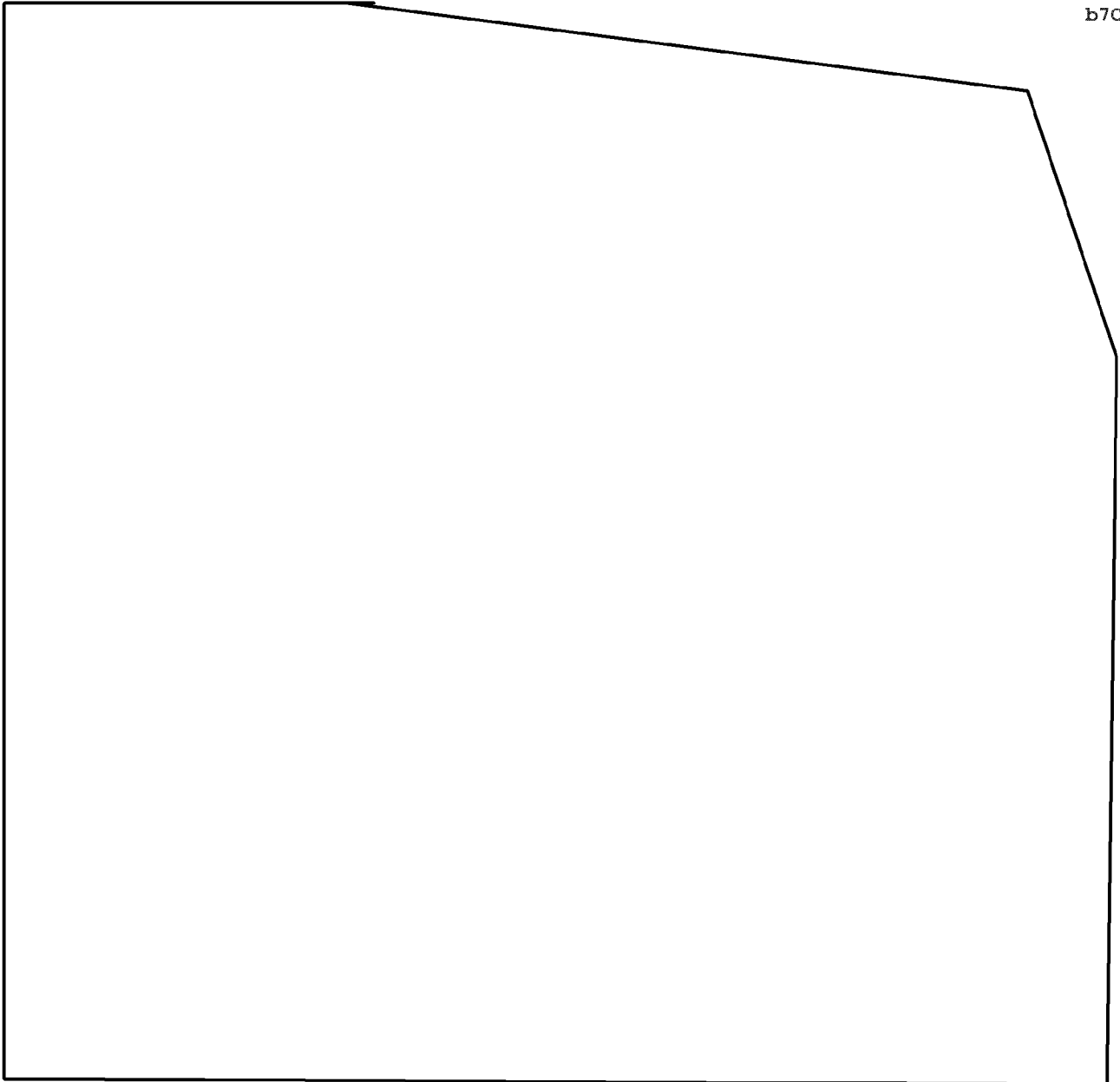
**Federal Bureau of Investigation**

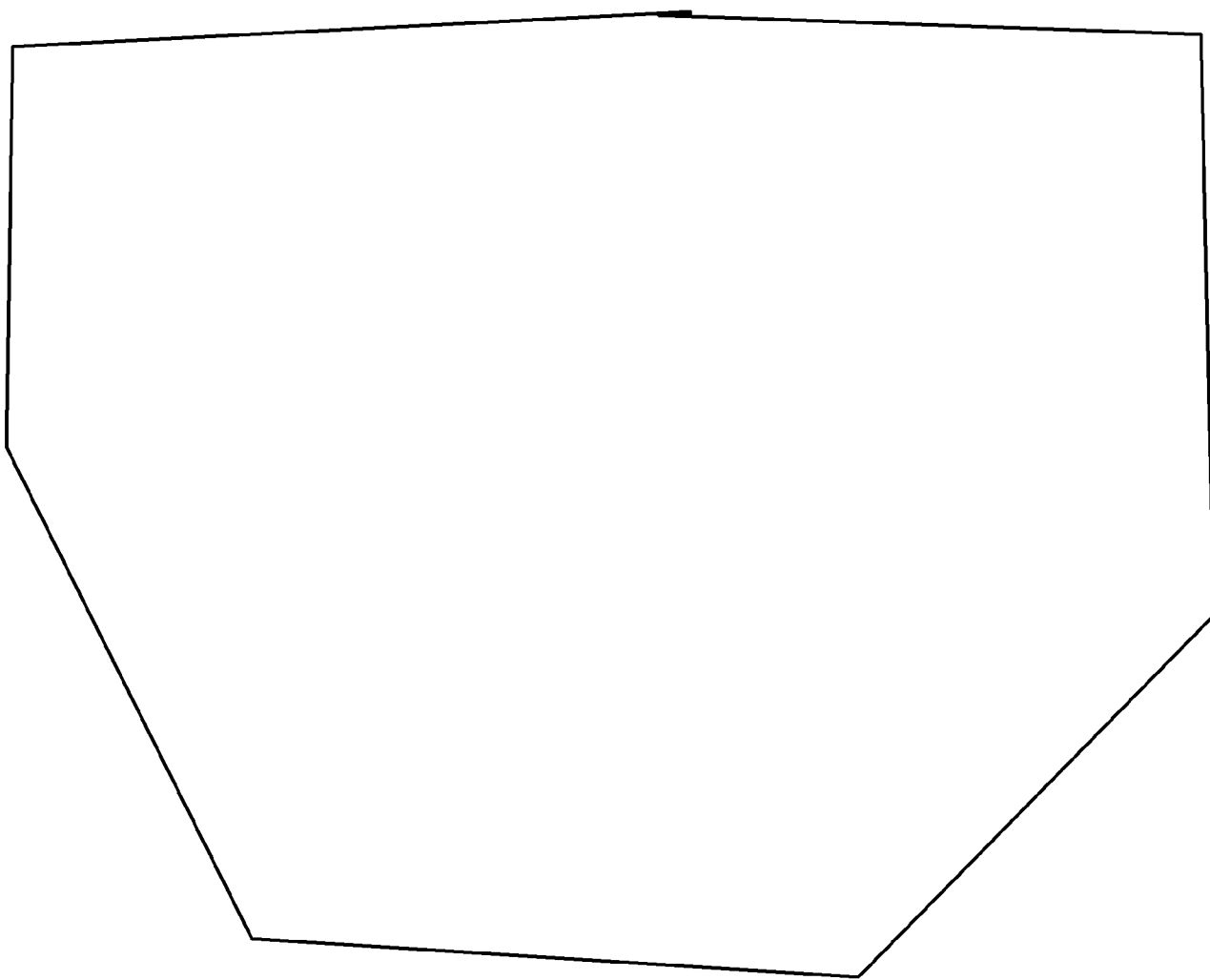
In Reply, Please Refer to  
File No.

b5

b6

b7C





b6

b7C

[REDACTED] (OGC) (FBI)

**From:** [REDACTED] (Div13) (FBI)  
**Sent:** Monday, May 10, 2004 7:09 AM  
**To:** [REDACTED] (Div09) (FBI)  
**Subject:** RE: Question on dissem of Grand Jury info to OIPR

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-03-2005 BY 65179 DMH/CLS  
CA# 05-CV-0845

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

[REDACTED]

Is a certain person at OIPR getting LHM's with FGJ info? The AUSA was looking for a specific name to add to the list. I said I'd check.

-----Original Message-----

**From:** [REDACTED] (Div09) (FBI)  
**Sent:** Wednesday, May 05, 2004 1:28 PM  
**To:** [REDACTED] (Div13) (FBI)  
**Subject:** RE: Question on dissem of Grand Jury info to OIPR

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

Yes, but this is disclosure of GJ info and according to the AGG (see EC from OGC dated 11/5/02) it must be marked if it identifies a USPER by name, nickname, etc. Most LHMs to OIPR don't contain GJ info. Yes, the AUSA has to notify the judge that the info will be shared with OIPR.

-----Original Message-----

**From:** [REDACTED] (Div13) (FBI)  
**Sent:** Wednesday, May 05, 2004 10:07 AM  
**To:** [REDACTED] (Div09) (FBI)  
**Subject:** RE: Question on dissem of Grand Jury info to OIPR

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

yes there is usper info, but we send usper info to OIPR all the time, thousands of LHMs.

So do we need the AUSA to pre-approve the dissemination of the FGJ info to OIPR?

-----Original Message-----

**From:** [REDACTED] (Div09) (FBI)  
**Sent:** Wednesday, May 05, 2004 10:03 AM  
**To:** [REDACTED] (Div13) (FBI)  
**Subject:** RE: Question on dissem of Grand Jury info to OIPR

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

Does the info in the LHM identify any USPER by name, etc.? If so, the info will have to be marked as containing USPER info.

6/9/2005

In addition, the AUSA will have to notify the court that GJ info is being disseminated to OIPR.

-----Original Message-----

**From:** [REDACTED] (Div13) (FBI)  
**Sent:** Wednesday, May 05, 2004 9:31 AM  
**To:** [REDACTED] (Div09) (FBI)  
**Subject:** RE: Question on dissem of Grand Jury info to OIPR

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

The LHM is the initiation of a PI notification.

-----Original Message-----

**From:** [REDACTED] (Div09) (FBI)  
**Sent:** Wednesday, May 05, 2004 9:24 AM  
**To:** [REDACTED] (Div13) (FBI)  
**Subject:** RE: Question on dissem of Grand Jury info to OIPR

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

Is this for an initiation or an annual LHM?

-----Original Message-----

**From:** [REDACTED] (Div13) (FBI)  
**Sent:** Wednesday, May 05, 2004 8:01 AM  
**To:** [REDACTED] (Div09) (FBI)  
**Subject:** Question on dissem of Grand Jury info to OIPR

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

[REDACTED]

We have received an OIPR [REDACTED]  
[REDACTED] in the matter were obtained via Grand Jury  
supoena. The paragraph goes on to quote [REDACTED]

[REDACTED]

Can this LHM be sent to OIPR with that grand jury info in it?

b2

b7E

**SENSITIVE BUT UNCLASSIFIED**

**SENSITIVE BUT UNCLASSIFIED**

**SENSITIVE BUT UNCLASSIFIED**

Message

DATE: 10-19-2005  
CLASSIFIED BY 65179 DMH/CLS  
REASON: 1.4 (C)  
DECLASSIFY ON: 10-19-2030

Page 1 of 3

CA# 05-CV-0845

[REDACTED] OGC) (FBI)

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

From: [REDACTED] (CTD) (FBI)

~~SECRET~~

Sent: Thursday, August 05, 2004 12:13 PM

To: [REDACTED] (SI) (FBI)

b6

Cc:

b7C

Subject: RE: a pending pen application

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

b5

b6

b7C

SSA [REDACTED]  
FBIHQ / CTD / ITOS II / PRGU

(o)  
(p)

b6

b7C

-----Original Message-----

From: [REDACTED] (SI) (FBI)

Sent: Thursday, August 05, 2004 11:47 AM

To: [REDACTED] (CTD) (FBI); [REDACTED] (CTD) (FBI)

Cc: [REDACTED] OGC) (FBI); [REDACTED] (SI) (FBI)

Subject: RE: a pending pen application

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

b5

b6

b7C

Thanks, [REDACTED]

SA [REDACTED]  
Springfield Division, Champaign RA

b6

~~SECRET~~

-----Original Message----- b7C

From: [REDACTED] (CTD) (FBI)

6/9/2005

**Sent:** Thursday, August 05, 2004 9:33 AM

~~SECRET~~

**To:** [redacted] (CTD) (FBI)

**Cc:** [redacted] (OGC) (FBI); [redacted] (SI) (FBI)

**Subject:** FW: a pending pen application

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

[redacted] (a.k.a. Mr. Pen Register) -

b6

b7C

Please contact case agent SA [redacted] and obtain an update re how FBI Springfield has handled the collection on this PR/TT. What is the current status?

[redacted]

b5

b6

b7C

I dunno. [redacted] court-authorized data obtained via an application which contained one (1) non-material good-faith error seems draconian to me. I do not think we should accept this remedy without serious discussion and consideration.

Thanks.

SSA [redacted]  
FBIHQ / CTD / ITOS II / PRGU

[redacted] (o)  
[redacted] (p)

b2

b6

b7C

-----Original Message-----

**From:** [redacted] (OGC) (OGA)

**Sent:** Thursday, August 05, 2004 9:54 AM

**To:** [redacted] (CTD) (FBI); [redacted] (SI) (FBI)

**Subject:** a pending pen application

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

(S)

[redacted]

b1

b5

b6

b7C

[redacted] I can be reached at [redacted] at OIPR (voice mail) or at the FBI at [redacted] (no voice mail).

b7A

[redacted] hope your move went well.

b2

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**

~~SECRET~~

6/9/2005

~~SECRET~~

SA [redacted]  
Springfield Division, Champaign RA

[redacted]

b6

b7C

-----Original Message-----

**From:** [redacted] (OGC) (FBI)  
**Sent:** Monday, August 09, 2004 2:50 PM  
**To:** [redacted] (SI) (FBI)  
**Subject:** RE: Pending pen register

~~SENSITIVE BUT UNCLASSIFIED~~  
~~NON-RECORD~~

[redacted]

Thanks, that's helpful. When did you learn about the need to change the subject's status? Also, do you happen to know why this has not been brought to the attention of the court for so long? Is it because the OIPR attorney was not able to have draft explanations to the court approved by James Baker? It sounds to me like you and FBIHQ passed along the information to OIPR in a timely fashion, but the delay in getting it to court is due to the situation at OIPR. Correct?

b6

b7C

-----Original Message-----

**From:** [redacted] (SI) (FBI)  
**Sent:** Monday, August 09, 2004 3:43 PM  
**To:** [redacted] (OGC) (FBI)  
**Subject:** RE: Pending pen register

~~SENSITIVE BUT UNCLASSIFIED~~  
~~NON-RECORD~~

[redacted]

(S)

b1

b6

b7C

b3

b7A

SA [redacted]  
Springfield Division, Champaign RA

[redacted]

-----Original Message-----

**From:** [redacted] (OGC) (FBI)  
**Sent:** Monday, August 09, 2004 2:33 PM  
**To:** [redacted] (SI) (FBI)  
**Subject:** Pending pen register

b6

b7C

~~SENSITIVE BUT UNCLASSIFIED~~  
~~NON-RECORD~~

[redacted]

~~SECRET~~

~~SECRET~~

b1

b5

b7A

b6

b7C

[redacted] is out on SL today and [redacted]

(S)

Thanks,

[redacted]  
NSLB

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

~~SECRET~~

6/9/2005



[redacted] (OGC) (FBI)

~~SECRET~~

**From:** [redacted] (Div13) (FBI)  
**Sent:** Monday, May 10, 2004 10:31 AM  
**To:** [redacted] (Div09) (FBI)  
**Subject:** RE: Pen register

DATE: 10-14-2005  
CLASSIFIED BY 65179 DMH/CLS  
REASON: 1.4 (C)  
DECLASSIFY ON: 10-14-2030  
CA# 05-CV-0845

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE

Okay, so if I understand it right. . . You approve of us sending it on to OIPR?

Thanks

-----Original Message-----

**From:** [redacted] (Div09) (FBI)  
**Sent:** Monday, May 10, 2004 10:28 AM  
**To:** [redacted] (Div13) (FBI)  
**Subject:** RE: Pen register

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

[redacted]

I really should take a look at those in the draft stage so that I can identify any potential legal issues prior to the application being sent to OIPR. Plus, under the new system I should be reviewing things before they are assigned to an OIPR attorney. After they are assigned, my role is limited. I intend to send something on procedures under this new system to everyone in PRGU soon.

b6

b7C

[redacted]

-----Original Message-----

**From:** [redacted] (Div13) (FBI)  
**Sent:** Monday, May 10, 2004 10:18 AM  
**To:** [redacted] (Div09) (FBI)  
**Subject:** FW: Pen register

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

[redacted]

This is in regards to the email you sent [redacted] We will get it to OIPR this week.

You won't need to do anything on it until OIPR gets through with it. Unless . . . according to the new AG thing, do you stick close to Pen Registers or not?

Thanks

b6

[redacted]

b7C

-----Original Message-----

**From:** [redacted] (Div13) (FBI)  
**Sent:** Monday, May 10, 2004 10:15 AM  
**To:** [redacted] (Div13) (FBI)

b6

b7C

~~SECRET~~

6/9/2005

~~SECRET~~**Subject:** RE: Pen register**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

You can start on it. Touch base with [ ] and let him know we are on it. It is one that we should go up on. He is the main guy in [ ] [ ]

-----Original Message-----

**From:** [ ] (Div13) (FBI)  
**Sent:** Monday, May 10, 2004 9:54 AM  
**To:** [ ] (Div13) (FBI)  
**Subject:** RE: Pen register

b2

b7E

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

Good lord, [ ] on it this week. I just got the application on Friday. The EC was dated 4/20. I haven't read it yet. Do you want to see it. And yes, I'll get it in the DB.

-----Original Message-----

**From:** [ ] (Div13) (FBI)  
**Sent:** Monday, May 10, 2004 9:49 AM  
**To:** [ ] (Div13) (FBI)  
**Subject:** FW: Pen register

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**

[ ] do you remember this request? It is possible that it happened while you were gone. If you don't remember it, I will check with [ ] Thanks. D

-----Original Message-----

**From:** [ ] (Div09) (FBI)  
**Sent:** Monday, May 10, 2004 9:38 AM  
**To:** [ ] (Div13) (FBI)  
**Subject:** Pen register

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**  
**NON-RECORD**~~SECRET~~

Hi [ ]

I received an EC from [ ] dated 4/20/04, requesting [ ]  
[ ] reviewed the request form and it is legally sufficient. Do you need me to do anything else on that? (S)

[ ]

b1

b2

~~SECRET~~

b7E

b6

b7C

**SENSITIVE BUT UNCLASSIFIED**~~SECRET~~

~~SECRET~~

[redacted] (OGC) (FBI)

b6

b7C

From: [redacted] CTD) (FBI)  
 Sent: Wednesday, September 01, 2004 12:14 PM  
 To: [redacted] (OGC) (FBI)  
 Cc: [redacted] (OGC) (FBI)  
 Subject: [redacted] (S)

DATE: 10-17-2005  
 CLASSIFIED BY 65179 DMH/CLS  
 REASON: 1.4 (C)  
 DECLASSIFY ON: 10-17-2030  
 CA# 05-CV-0845

b1

~~SECRET~~  
 RECORD [redacted] (S)

ALL INFORMATION CONTAINED  
 HEREIN IS UNCLASSIFIED EXCEPT  
 WHERE SHOWN OTHERWISE

b1

b2

b7E

b6

b7C

[redacted]  
 I just got this [redacted] which we hope is in final form [redacted] (S)

I'm working with [redacted] at OIPR on this, so if you could include him on the results, he should be able to get this to [redacted] on Friday.

Thanks,

[redacted]

b2

SSA [redacted]

b7E

b6

b7C

~~DERIVED FROM: Multiple Sources~~  
~~DECLASSIFY ON: 20290901~~  
~~SECRET~~

~~SECRET~~

6/17/2005

Refer to DOJ, OIPR

**SECRET**

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D. C.

IN RE ABDULMALEK SABRAGH, :

A U.S. PERSON. (S) : Docket Number: PR/TT

**APPLICATION FOR PEN REGISTER AND/OR TRAP AND TRACE DEVICES  
FOR FOREIGN INTELLIGENCE PURPOSES**

The United States of America, through the undersigned Department of Justice attorney, hereby applies to this Court, pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), §§ 1801-1811, 1841-1846, as amended by the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA PATRIOT Act), Public Law 107-56, for an order authorizing the installation and use of pen register and/or trap and trace device(s) to protect against

**SECRET**

Classified by: James A. Baker, Counsel for  
Intelligence Policy, OIPR, DOJ  
Reason: 1.4(c)  
Declassify on: X1

Refer to DOJ, OIPR

**SECRET**

international terrorism in an investigation concerning Abdulmalek Sabbagh, a United States person, which is being conducted by the Federal Bureau of Investigation (FBI). (S)

1. The Counsel for Intelligence Policy<sup>1</sup> is authorized to approve applications for pen register and/or trap and trace surveillance under the Act. The Counsel's approval of this application and finding that it satisfies the criteria and requirements for such applications are set forth below. (U)

2. The federal officer seeking to use the pen register and/or trap and trace device(s) covered by this application is Douglas E. Lindquist, Supervisory Special Agent of the FBI assigned to the Palestinian Rejectionist Groups Unit (PRGU) of the International Terrorism Operations Section 2 (ITOS 2) in the FBI's Counterterrorism Division of FBI Headquarters in Washington, D.C., whose official duties include supervision of the FBI's investigation of Abdulmalek Sabbagh. (S)

3. Set forth below is the certification of the applicant that the information likely to be obtained from this pen register and/or trap and trace surveillance is relevant to an ongoing investigation of a United States person to protect

---

<sup>1</sup> Attorney General Order Number 2569-2002, dated March 26, 2002, a copy of which is on file with this Court. (U)

**SECRET**

**SECRET**

against international terrorism that is not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution.<sup>2</sup> (U)

4. Abdulmalek Sabbagh is the subject of a full FBI National Security investigation, which was initiated on November 6, 2003. He is a U.S. citizen who was naturalized on June 2, 2000. This investigation is being conducted on the basis of activities of Abdulmalek Sabbagh, a United States person, and not solely on the basis of activities of Sabbagh that are protected by the First Amendment to the Constitution. (S)

Since its initiation in late 2003, the FBI's investigation of Sabbagh has revealed that between December 28, 1994, and October 15, 2002, Sabbagh wired from the U.S. more than \$2,200,000 to accounts outside the U.S., including accounts in

---

<sup>2</sup> Section 214 of the USA PATRIOT Act provides that each application shall include:

a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

Section 402(c)(2) of FISA, 50 U.S.C. § 1842(c)(2), amended by USA PATRIOT Act of 2001, § 214 (2001), Pub. L. No. 107-56. (U)

**SECRET**

Refer to DOJ, OIPR

**SECRET**

Germany and Jordan. More specifically, FBI investigation to date has revealed that between 1994 and 2002, Sabbagh has made payments totaling approximately \$240,000, to "Islamic Relief Worldwide," "Life for Relief and Development,"<sup>3</sup> and "Holy Land Foundation," all organizations that FBI investigation has implicated in supplying funds to HAMAS.<sup>4</sup> (S)

FBI investigation has also determined that on or about November 27, 2000, Sabbagh was in telephonic contact with Mohammad El-Mezain, the subject of an FBI (San Diego, California) full National Security investigation and a former target of Court-authorized electronic surveillance as a suspected HAMAS fund-raiser active within the U.S. On July 27, 2004, El-Mezain was charged in federal Court in Dallas, Texas, with crimes

---

<sup>3</sup> Life for Relief and Development is the current target of Court-authorized electronic surveillance as a suspected agent of Iraq, and a former target of Court-authorized electronic surveillance as an agent of HAMAS (described below) involved in raising funds for HAMAS. (S)

<sup>4</sup> FBI and Central Intelligence Agency (CIA) investigations in this and in other matters have revealed that HAMAS is a terrorist organization that espouses an extremist Islamic fundamentalist ideology and maintains support structures in the United States, Britain, France, Italy, Germany, and Jordan. CIA reporting also indicates that HAMAS has active support structures in Iran, Kuwait, Sudan, Syria, and Yemen. HAMAS terrorist attacks have resulted in scores of deaths and hundreds of injuries in Israel, including the killing of several U.S. citizens. (S)

**SECRET**

Refer to DOJ, OIPR

**SECRET**

related to allegations that he has funneled money to HAMAS in support of its terrorist activities. (S)

Additionally, FBI investigation has revealed that between August 1999 and February 2000, six calls to Sabbagh's home telephone number were made by Mohamad Kawam, the subject of a current FBI full National Security investigation as a suspected leader of a HAMAS financial support network in New Jersey. Additionally, a source considered reliable by the FBI reported that on or about March 12, 2003, and on or about August 4, 2002, Kawam was in telephone contact with El-Mezain (described above). (S)

5. This is the initial application for pen register and trap and trace surveillance of the target of this application. (S)

6. The telephone line(s) and/or other facility/ies to which the requested pen register and/or trap and trace device(s) is/are to be attached or applied is/are:

(A) (304) 842-2666, which is leased by or listed to Ghayda Salkini, 102 Allison Avenue, Bridgeport, West Virginia;<sup>5</sup>

---

<sup>5</sup> FBI investigation has revealed that Sabbagh informed a local utility that (304) 842-2666 is his home telephone number. The Morgantown (West Virginia) Mosque telephone directory

**SECRET**



**SECRET**

(B) (304) 622-2500, which is leased by or listed to Abdulmalek Sabbagh, M.D., 4 Hospital Plaza, Suite 302, Clarksburg, West Virginia;<sup>6</sup>

(C) (304) 269-1448, which is leased by or listed to Abdulmalek Sabbagh, M.D., Route 4, Box 9-A, Weston, West Virginia;<sup>7</sup>

(D) (304) 269-5235, a facsimile machine, which is leased by or listed to Abdulmalek Sabbagh, M.D., Route 4, Box 9-A, Weston, West Virginia;

(E) (304) 269-1400, which is leased by or listed to Ghayda Salkini, Sabbagh's wife, Route 4, Box 9-A, Weston, West Virginia. (S)

The FBI has verified the information in subparagraph (A) above through its investigation, as described above. The FBI has verified the information in subparagraphs (B), (C), and (E) above through a National Security Letter and through newspaper

---

ascribes this number to Sabbagh, and www.infospace.com, an Internet telephone directory, provides this number as being subscribed to by Sabbagh's wife, Ghayda Salkini, at 102 Allison Avenue, Bridgeport, West Virginia, which FBI investigation has revealed is Abdulmalek Sabbagh's home address. (S)

<sup>6</sup> FBI investigation has revealed that Sabbagh maintains a medical practice at this address. (S)

<sup>7</sup> FBI investigation has revealed that Sabbagh also maintains a medical practice at this address. (S)

**SECRET**

**SECRET**

advertisements for Sabbagh's medical practices. The FBI has verified the information in subparagraph (D) above through a National Security Letter. (S)

7. This request is for pen register and/or trap and trace authority within the United States. (S)

8. The Court is requested to authorize the installation and use of pen register and/or trap and trace (including caller identification details regarding incoming calls) device(s), with no geographical limits or restrictions within the United States, for a period of ninety days and to direct that the following person(s) furnish the FBI with any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register and/or trap and trace device(s) in such a manner as will protect its secrecy and produce a minimum amount of interference with the services each such person is providing to their subscriber:  
Verizon West Virginia, Inc. (S)

WHEREFORE, the United States submits that this application satisfies the criteria and requirements of the Act,

**SECRET**

Refer to DOJ, OIPR

**SECRET**

as amended, and therefore requests that this Court authorize the installation and use of the pen register and/or trap and trace device(s) described herein, and enter the proposed orders that accompany this application. (U)

Respectfully submitted,

\_\_\_\_\_  
Kevin A. Forder  
Attorney  
U.S. Department of Justice

**VERIFICATION**

I declare under penalty of perjury that the facts set forth in the foregoing application are true and correct.

Executed pursuant to Title 28, United States Code, § 1746, on

\_\_\_\_\_. (U)

\_\_\_\_\_  
Douglas E. Lindquist  
Supervisory Special Agent  
Federal Bureau of Investigation

**SECRET**

Refer to DOJ, OIPR

**SECRET**

**CERTIFICATION**

I certify that the information likely to be obtained from the pen register and/or trap and trace device(s) requested in this application regarding Abdulmalek Sabbagh is relevant to an ongoing investigation of a United States person to protect against international terrorism that is not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution. (S)

---

Kevin A. Forder  
Attorney  
U.S. Department of Justice

**SECRET**

Refer to DOJ, OIPR

**SECRET**

**DESIGNATED ATTORNEY APPROVAL**

I find that this application regarding **Abdulmalek Sabbagh** satisfies the criteria and requirements for such applications set forth in the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801-1811, 1841-1846, as amended, and hereby approve its filing with the Foreign Intelligence Surveillance Court. (S)

\_\_\_\_\_  
James A. Baker  
Counsel for Intelligence Policy

\_\_\_\_\_  
Date

**SECRET**

[REDACTED] (OGC) (FBI)

**From:** [REDACTED] (Div09) (FBI)  
**Sent:** Wednesday, March 24, 2004 11:31 AM  
**To:** [REDACTED] (Div09) (FBI)  
**Subject:** RE: obtaining tax info

ALL INFORMATION CONTAINED  
 HEREIN IS UNCLASSIFIED b6  
 DATE 10-19-2005 BY 65179 DMH/CLS b7C  
 CA# 05-CV-0845

**UNCLASSIFIED**  
**NON-RECORD**

[REDACTED]

b5

But you can review the relevant sections yourself and see if you find something that I overlooked.

[REDACTED]

b6  
 b7E

-----Original Message-----

**From:** [REDACTED] (Div09) (FBI)  
**Sent:** Wednesday, March 24, 2004 9:46 AM  
**To:** [REDACTED] (Div09) (FBI)  
**Subject:** RE: obtaining tax info

b6  
 b7C

**UNCLASSIFIED**  
**NON-RECORD**

[REDACTED]

b6  
 b7C  
 b5

-----Original Message-----

**From:** [REDACTED] (Div09) (FBI)  
**Sent:** Wednesday, March 24, 2004 9:42 AM  
**To:** [REDACTED] (Div09) (FBI)  
**Subject:** RE: obtaining tax info

b6  
 b7C

**UNCLASSIFIED**  
**NON-RECORD**

[REDACTED]

b6  
 b7C  
 b5  
 b2  
 b7E

6/17/2005

-----Original Message-----

**From:** [REDACTED] (Div09) (FBI)  
**Sent:** Tuesday, March 23, 2004 3:51 PM  
**To:** [REDACTED] (Div09) (FBI)  
**Subject:** obtaining tax info

b6

b7C

UNCLASSIFIED  
NON-RECORD

b2

b7E

b5

Thanks.

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

**FBI FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)  
BUSINESS RECORDS REQUEST FORM**

**INSTRUCTIONS**

The FBI must use this form to request that the National Security Law Branch (NSLB) prepare an application to the Foreign Intelligence Surveillance Court (FISC) for a Business Records Order, pursuant to the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §1861.

FBI field offices must adhere to the following procedures in using this form:

- (1) The FBI special agent (SA) in the relevant FBI field office/division with primary responsibility for the foreign counterintelligence or counterterrorism investigation to which the request relates should complete this form.
- (2) This form must be reviewed and approved by Supervisory Special Agent (SSA), the Chief Division Counsel (CDC), and the Special Agent in Charge (SAC) or the Program Assistant Special Agent-in-Charge(ASAC).
- (3) This form should be sent to the appropriate FBI Headquarters division (Counterintelligence or Counterterrorism), the National Security Law Branch (NSLB), Room 7975, and the FISA Unit, Room 1B046.

Based on the information provided on this form, NSLB will prepare a FISA Business Records Application, and Order and present it to the FISC.

Direct any questions about how to complete this form to the FBI HQ SSA or NSLB (202) 324-3951.

Blank versions of this form are unclassified. **Add classification markings to the form according to the classification of the information you provide.**

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-17-2005 BY 65179 DMH/CLS

CA# 05-CV-0845



**FISA REQUEST FOR ACCESS TO BUSINESS RECORDS,  
I.E., "ANY TANGIBLE THING (INCLUDING BOOKS, RECORDS,  
PAPERS, DOCUMENTS AND OTHER ITEMS)" (50 USC Section 1861)**

**1. General Information**

- a. **Name of Subject(s) of the investigation for which the tangible things are sought:**
- b. **FBI file number(s):**
- c. **Date full investigation or preliminary investigation of such subject was authorized:**
- d. **Office of origin:**

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-19-2005 BY 65179 DMH/CLS  
CA# 05-CV-0845
- e. **Case Agent Point of Contact:**
  - i. **Name:**
  - ii. **Telephone:**
  - iii. **Secure Fax:**
- f. **FBI Headquarters SSA:**
  - i. **Name:**
  - ii. **Telephone:**
  - iii. **Secure Fax:**
- g. **Status of Subject of the Investigation**
  - i. **USP**
  - ii. **Non-USP or**
  - iii. **Foreign power**
- h. **Status of Subject of the Request, if different from Subject of the Investigation**
  - i. **USP**
  - ii. **Non-USP**
  - iii. **Foreign Power**

**2. Basis of Request for Tangible Things**

- a. **Specifically describe the tangible things (e.g. books, records, papers, documents) you are requesting. If the tangible thing is not a written document (e.g., an apartment key), explain why you believe that it is being kept by a custodian in the normal course of business. Note that the subject of the request does not have to**

be the subject of the investigation.

- b. If relevant, state whether you are requesting the original or copy of the tangible things.
- c. Provide a brief summary of the full investigation or preliminary investigation for which the requested tangible things are sought.
- d. Explain the manner in which the requested tangible things are expected to provide foreign intelligence information for the full investigation or preliminary investigation.

3. Service of the Business Records Order

- a. Identify the current custodian, owner, or person in possession of the requested tangible things.
- b. Identify the name, address, title, and telephone number of any custodian or person to whom an order needs to be directed to require the production of the requested tangible things.

4. Field Office Approval

I have reviewed this request and certify that the requested tangible things are sought for an authorized investigation, conducted in accordance with the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations, to obtain foreign intelligence not concerning a USPER or to protect against international terrorism or clandestine intelligence activities. I further certify that the authorized investigation is not being conducted solely upon the basis of activities protected by the First Amendment of the Constitution.

Supervisory Special Agent (SSA) approving this form:

Printed (or Typed) Name:

Telephone Number:

Signature:

Date:

---

(Classification of completed form)

**CDC approving this form:**

**Printed (or Typed) Name:**

**Telephone Number:**

**Signature:**

**Date:**

**SAC or Program ASAC approving this form:**

**Printed (or Typed) Name:**

**Telephone Number:**

**Signature:**

**Date:**

---

(Classification of completed form)

FEDERAL BUREAU OF INVESTIGATION  
FOIPA  
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 8  
Page 157 ~ Referral/Direct  
Page 158 ~ Referral/Direct  
Page 159 ~ Referral/Direct  
Page 160 ~ Referral/Direct  
Page 161 ~ Referral/Direct  
Page 162 ~ Referral/Direct  
Page 163 ~ Referral/Direct  
Page 164 ~ Referral/Direct